#2

Docket No. 1460.1006/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yusaku FUJII et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: May 31, 2000

For: METHOD AND EQUIPMENT FOR ENCRYPTING/DECRYPTING....

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. Hei11-174648
Filed: June 12, 1999

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: May 31, 2000

By: _____

H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

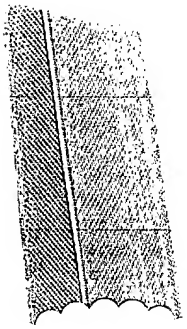
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

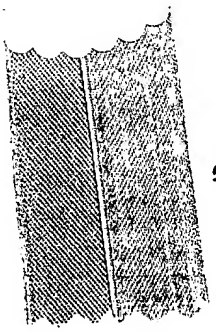
出 願 年 月 日
Date of Application: １９９９年 ６月２１日

出 願 番 号
Application Number: 平成１１年特許願第１７４６４８号

出 願 人
Applicant (s): 富士通株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年 ２月１８日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３００７２８７

【書類名】　特許願

【整理番号】　9805752

【提出日】　平成11年 6月21日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 9/00 671

【発明の名称】　生体情報の暗号化・復号化方法および装置並びに、生体情報を利用した本人認証システム

【請求項の数】　13

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　藤井　勇作

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　新崎　卓

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100072718

【弁理士】

【氏名又は名称】　古谷　史旺

【電話番号】　3343-2901

【選任した代理人】

【識別番号】　100075591

【弁理士】

【氏名又は名称】　鈴木　榮祐

【手数料の表示】

【予納台帳番号】　013354

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704947

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　生体情報の暗号化・復号化方法および装置並びに、生体情報を利用した本人認証システム

【特許請求の範囲】

【請求項１】　個人に固有の特徴を表す生体情報の入力を受け、

暗号化の都度、任意の値を持つ数値キーを決定し、

前記数値キーと所定の一次鍵とから暗号鍵を生成し、

前記暗号鍵を用いて前記生体情報を暗号化し、

得られた暗号化生体情報と前記数値キーとに基づいて、復号化処理側で暗号鍵を再生するための復号制御情報を作成し、

前記暗号化生体情報と前記復号制御情報とを組み合わせて認証情報を作成することを特徴とする生体情報暗号化方法。

【請求項２】　暗号化生体情報と復号制御情報との組み合わせを受け取り、

前記暗号化生体情報と復号制御情報とに基づいて、暗号化処理側において暗号鍵の生成に用いられた数値キーを復元し、

前記数値キーと所定の一次鍵とに基づいて、暗号化処理側において用いられた暗号鍵を復元し、

前記暗号鍵を用いて前記暗号化生体情報を復号化し、生体情報を復元する

ことを特徴とする生体情報復号化方法。

【請求項３】　個人に固有の特徴を表す生体情報を入力する生体情報入力手段と、

前記生体情報を暗号化する度に、任意の値を持つ数値キーを決定する数値キー決定手段と、

前記数値キーと所定の一次鍵とに基づいて暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵を用いて、入力された生体情報を暗号化する第１暗号化手段と、

前記第１暗号化手段によって得られた暗号化生体情報と前記数値キーとに基づいて、復号化処理側で暗号鍵を再生するために用いる復号制御情報を作成する制御情報作成手段と、

前記暗号化生体情報と前記復号制御情報とを組み合わせた認証情報を作成する作成手段と

を備えたことを特徴とする生体情報暗号化装置。

【請求項４】　生体情報を所定の暗号化方法に従って暗号化して得られる暗号化生体情報と復号処理に用いる復号制御情報とを含む認証情報を受け取る受取手段と、

前記認証情報に含まれる暗号化生体情報と復号制御情報とに基づいて、暗号化鍵の生成に用いられた数値キーを作成する数値キー復元手段と、

前記数値キーと所定の一次鍵とに基づいて、暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵を用いて暗号化生体情報を復号化する第１復号化手段と

を備えたことを特徴とする生体情報復号化装置。

【請求項５】　個人に固有の特徴を表す生体情報を入力する生体情報入力手順と、

前記生体情報を暗号化する度に、無作為に任意の数値キーを決定する数値キー決定手順と、

前記数値キーと所定の一次鍵とに基づいて暗号鍵を生成する暗号鍵生成手順と、

前記暗号鍵を用いて、入力された生体情報を暗号化する第１暗号化手順と、

前記第１暗号化手順において得られた暗号化生体情報と前記数値キーとに基づいて、復号化処理側で暗号鍵を再生するために用いる復号制御情報を作成する制御情報作成手順と、

前記暗号化生体情報と前記復号制御情報とを組み合わせた認証情報を作成する作成手順と

をコンピュータに実行させるプログラムを記録した記憶媒体。

【請求項６】　生体情報を所定の暗号化方法に従って暗号化して得られる暗号化生体情報と復号処理に用いる復号制御情報とを含む認証情報を受け取る受取手順と、

前記認証情報に含まれる暗号化生体情報と復号制御情報とに基づいて、暗号化

鍵の生成に用いられた数値キーを作成する数値キー復元手順と、

前記数値キーと所定の一次鍵とに基づいて、暗号鍵を生成する暗号鍵生成手順と、

前記暗号鍵を用いて暗号化生体情報を復号化する第１復号化手順と

をコンピュータに実行させるプログラムを記録した記憶媒体。

【請求項７】　個人に固有の特徴を表す生体情報の入力を受け、

前記生体情報を構成する各要素について、その前後を含む所定の範囲に含まれる複数の要素を引数とする所定の関数を用いて数値変換することによって、前記生体情報をスクランブルし、

スクランブルされた生体情報を所定の暗号鍵を用いて暗号化する

ことを特徴とする生体情報の暗号化方法。

【請求項８】　暗号化生体情報を受け取り、

前記暗号化生体情報を所定の暗号鍵を用いて復号化し、

復号結果に含まれる各要素に含まれる元の複数の要素の寄与分を分離してスクランブルを解除し、生体情報を復元する

ことを特徴とする生体情報の復号化方法。

【請求項９】　個人に固有の特徴を表す生体情報を入力する生体情報入力手段と、

前記生体情報の入力に応じて、前記生体情報を構成する各要素を含む複数の要素を引数とする所定の関数を用いて数値変換するスクランブル手段と、

前記スクランブル手段による変換結果を所定の暗号鍵を用いて暗号化する第２暗号化手段と

を備えたことを特徴とする生体情報暗号化装置。

【請求項１０】　生体情報をスクランブルした後に暗号化して得られる暗号化生体情報を受け取って、所定の暗号鍵を用いて復号化する第２復号化手段と、

復号結果を所定の関数を用いて数値変換することによって、暗号化処理において施されたスクランブルを解除するスクランブル解除手段と

を備えたことを特徴とする生体情報復号化装置。

【請求項１１】　個人に固有の特徴を表す生体情報を入力する生体情報入力

手順と、

前記生体情報を暗号化する度に、前記生体情報を構成する各要素を含む複数の要素を引数とする所定の関数を用いて数値変換するスクランブル手順と、

前記スクランブル手順による変換結果を所定の暗号鍵を用いて暗号化する第２暗号化手順と

をコンピュータに実行させるプログラムを記録した記憶媒体。

【請求項１２】　生体情報をスクランブルした後に暗号化して得られる暗号化生体情報を受け取って、所定の暗号鍵を用いて復号化する第２復号化手順と、

復号結果を所定の関数を用いて数値変換することによって、暗号化処理において施されたスクランブルを解除するスクランブル解除手順と

をコンピュータに実行させるプログラムを記録した記憶媒体。

【請求項１３】　認証クライアント装置と認証サーバ装置とがネットワークを含む伝送媒体を介して暗号化した認証情報を授受して、本人認証処理に供する遠隔本人認証システムにおいて、

認証クライアント装置は、

個人に固有の特徴を表す生体情報を入力する生体情報入力手段と、

利用者が自身の資格を証明するための資格情報として、他者に公開されている識別情報と他者からは秘匿されるべきパスワードとを含む情報を入力する資格情報入力手段と、

前記パスワードを暗号鍵として、前記生体情報を暗号化する第３暗号化手段と、

前記第３暗号化手段によって得られた暗号化生体情報と前記識別情報との組み合わせを認証情報として前記伝送媒体に出力する出力手段とを備えた構成であり、

認証サーバ装置は、

全ての利用者に対応する識別情報に対応して、パスワードと該当する個人の生体的な特徴を計測して得られた標準情報とを登録する資格情報登録手段と、

前記伝送媒体を介して、前記暗号化生体情報と前記識別情報との組み合わせを受け取る入力手段と、

前記入力手段を介して受け取った識別情報に基づいて、前記資格情報登録手段から該当するパスワードおよび標準情報を検索する検索手段と、

前記検索手段を介して受け取ったパスワードを暗号鍵として、前記入力手段から受け取った暗号化生体情報を復号化する第３復号化手段と、

前記第３復号化手段によって復元された生体情報と前記検索手段によって検索された標準情報とを照合する照合手段とを備えた構成である

ことを特徴とする遠隔本人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、指紋や声紋などのように個人に固有な特徴を表す生体情報に適合した生体情報暗号化・復号化方法及び装置並びに、生体情報に基づいて、ネットワークを介して本人を認証するための遠隔本人認証システムに関するものである。

指紋や声紋、虹彩パターンなどは、個人に固有な特徴でありまた個人の生涯を通して不変であることから、本人を認証するための情報として優れており、入退室管理システムのような様々な本人認証システムに利用されている。

その一方、パーソナルコンピュータなどの情報関連機器の普及に伴って、一般の利用者の間でも、ネットワークを介して様々な情報の授受が盛んに行われるようになっており、ネットワークを介した商取引や文書のやりとりなどの重要性が高まっている。

商取引や重要な文書の交換などをネットワークを介して適切に行うために、ネットワークを介して互いを証明する情報を授受し、相互に本人を確実に認証する技術が必要とされており、本人を確認するための情報として生体情報が注目されている。

【０００２】

【従来の技術】

図１５に、従来のネットワークを介した遠隔個人認証システムの構成図を示す。

図１５に示した遠隔本人認証システムにおいて、認証クライアント装置４１０

は、ネットワークを介して認証情報を送出し、認証サーバ装置４２０は、受け取った認証情報と登録された認証情報とを照合した結果に基づいて、認証クライアント装置４１０の利用者の利用資格を認証する構成となっている。

【０００３】

例えば、パソコン通信サービスなどを利用する際には、利用者のパソコンが認証クライアント装置となり、サービス提供者側のホストコンピュータが認証サーバ装置となる。

【０００４】

この場合に、利用者がキーボード４１１を介して入力したユーザＩＤおよびパスワードに基づいて、依頼制御部４１２によって認証情報が作成され、通信制御部４１３を介してネットワークに送出される。

このとき、暗号化部４１４により、上述したパスワードを暗号化し、依頼制御部４１２による認証情報作成処理に供する構成とすることにより、ネットワークを介して認証サーバ装置４２０に安全にパスワードを渡すことができる。

【０００５】

図１５に示した認証サーバ装置４２０において、復号化部４２１は、通信制御部４２２を介して暗号化されたパスワードを受け取り、これを復号化してパスワードを復元し、認証制御部４２３の処理に供する構成となっている。

一方、認証制御部４２３は、通信制御部４２２を介して受け取ったユーザＩＤに基づいて、パスワードデータベース４２４から登録されたパスワードを検索し、この登録されたパスワードと復号化部４２１によって復元されたパスワードとを照合する構成となっている。

【０００６】

この場合は、復元されたパスワードと登録されたパスワードとが一致した場合に、本人であると確認した旨の認証結果が通信制御部４２２を介して認証クライアント装置４１０側に通知され、これに応じて、依頼制御部４１２は、認証結果を示すメッセージを作成し、ＣＲＴディスプレイ装置（ＣＲＴ）４１５を介して利用者に利用資格が承認された旨を通知している。

【０００７】

また、図１５に示すように、暗号化部４１４が、時計４１６から受け取った現在時刻を用いてパスワードを暗号化し、復号化部４２１が、時計４２５から受け取った現在時刻を用いて復号化する構成とする場合もある。

この場合は、利用者が入力したパスワードを毎回異なる暗号に変換することができるので、ネットワークを介してパスワードをより安全に送受信することができる。

【０００８】

このような遠隔本人認証システムにおいては、利用者が入力するパスワードが、利用者本人を証明する情報となっており、本人を確実に認証し、他者を排除するためには、個々の利用者がパスワードを適切に管理していることが必要である。

一方、生体情報は、個人に固有のものであるから、本人を証明する情報として優れており、指紋などの生体情報は、例えば、入退室管理システムなどにおいて、その場にいる人物についての近接本人認証システムの認証情報として利用されている。

【０００９】

図１６は、生体情報を利用した本人認証システムの構成例を示す図である。

例えば、生体情報として指紋データを用いる場合は、図１６に示すように、本人認証システムは、指紋データ測定装置４３０と指紋照合装置４４０とから構成され、この指紋データ測定装置４３０によって、その場にいる人物の指紋の特徴を測定し、この測定結果を一連の数値データの集まりによって表した指紋データを認証制御部４０１を介して指紋照合装置４４０による照合処理に供する構成となっている。

【００１０】

図１６に示した指紋データ測定装置４３０において、特徴抽出部４３１は、指紋読取部４３２によって読み取られた画像データを受け取り、この画像データによって表された指紋の特徴を抽出し、指紋データ作成部４３３の処理に供する構成となっている。

この指紋データ作成部４３３は、特徴抽出部４３１によって抽出された特徴情

報を所定の形式に従って配列して指紋データを形成し、認証制御部４０１に渡す構成となっている。

【００１１】

一方、図１６に示した指紋照合装置４４０において、指紋データベース４４１は、入室資格を持つ各個人に割り当てられたユーザＩＤに対応してそれぞれの指紋データを標準データとして登録しており、指紋データ検索部４４２は、利用者がキーボード４０２を介して入力したユーザＩＤを認証制御部４０１を介して受け取り、このユーザＩＤに対応する指紋データを検索して、照合判定部４４３の処理に供する構成となっている。

【００１２】

ここで、指紋に限らず、一般に、生体情報を数値として計測した場合には、測定の際の条件（圧力、温度）などによって、測定の都度にその値が変動する。

例えば、指の押しつけ圧力や指の温度、周囲の湿度などによって、読み取られる画像データは微妙に変化し、これに伴って、指紋の隆線の形状や端点および分岐点の分布が変動する。

【００１３】

したがって、照合判定部４４３は、必要とされる認識率に応じて、入力された指紋データの所定の範囲が、標準データの該当する範囲のデータと一致するか否かによって、入力された指紋データが本人のものであるか否かを判定している。

図１７に、生体情報を照合する処理を説明する図を示す。

例えば、百人に一人程度の誤認識を許容する用途では、照合判定部４４３は、図１７(ａ)に注目範囲として示したように、指紋データのごく一部に対応する範囲について、標準データと入力された指紋データとを比較し、この注目範囲に含まれる全ての要素が所定の誤差の範囲内で一致しているか否かを示す判定結果を認証制御部４０１に返せばよい。

【００１４】

例えば、図１７(ａ)において斜線を付して示す範囲において、標準データと入力された指紋データとが誤差範囲内で一致している場合に、照合判定部４４３は、入力された指紋データと本人の指紋データとが一致している旨の判定結果を認

証制御部４０１に送出すればよい。

これに応じて、認証制御部４０１は、その場にいる人物を本人と認証し、表示部４０３を介して入室を許可する旨を通知するとともに、入退室制御部４０４を介してドアのロックを解除するなどの必要な制御を行えばよい。

【００１５】

一方、図１７(ｂ)に示すように、上述した注目範囲に含まれる要素の一部に許容誤差を超える不一致があった場合に、照合判定部４４３は、標準データと入力された指紋データとが一致しない旨の判定結果を送出し、これに応じて、認証制御部４０１は、その場にいる人物の入室を拒否するために必要な制御を行えばよい。

【００１６】

ここで、図１７(ａ)に示したように、比較的狭い範囲を注目範囲として、指紋データの照合を行った場合は、百人に一人程度の誤認識が発生する代わりに、指紋データを測定する条件が悪い場合においても、本人を誤って排除してしまう可能性を低くすることができる。

その一方で、一万人に一人程度の誤認識率を必要とする用途では、図１７(ｃ)に示すように、指紋データの大半を注目範囲に含める必要がある。

【００１７】

この場合は、資格を持たない人物を誤って本人と認証してしまう危険性を低くすることができる反面、資格を持つ人物であっても、指先のわずかな汚れのために、拒絶してしまう可能性が増大する。なぜなら、注目範囲が広くなればなるほど、入力した指紋データと標準データとの間に許容誤差を超える不一致が生じている可能性が大きくなるからである。

【００１８】

ところで、一般に、ネットワークを介して情報を安全に伝送するための技術として、公開鍵方式を実現するためのＲＳＡアルゴリズムや共通鍵方式を適用したＤＥＳ(data encryption standard)方式が既に実用化されている。

ＤＥＳ方式は、暗号化対象の情報を56ビット単位のブロックに分割し、換字式暗号や転置式暗号を複雑に組み合わせて各ブロックを変換する暗号化方法であり

、変換の単位がブロックであることから、ブロック暗号化方式と呼ばれている。

【００１９】

【発明が解決しようとする課題】

上述した従来の遠隔本人認証システムでは、本人であることを証明する情報であるパスワードは、基本的に個々の利用者の管理に任されている。

しかしながら、パスワードの盗用を防ぐためには、パスワードが十分な長さであるとともに、パスワード自体は意味を持たない文字や記号の羅列であることが求められており、かつ、頻繁に変更することが必要であるため、個々の利用者がパスワードを適切に管理することは非常に困難である。

【００２０】

なぜなら、人間が、意味のない文字や記号の羅列を記憶することは難しく、しかも、頻繁に変更することは、利用者に多大な負担であるからである。

このため、多くの利用者が、公開されている個人情報や好んでアクセスする情報の種類などから容易に類推可能なパスワードを登録していたり、記憶する代わりにメモなどに記録して携帯しており、また、パスワードの変更を長期間に渡って怠っている場合も多い。

【００２１】

したがって、本人を認証する情報としてパスワードのみを用いる遠隔本人認証システムでは、ネットワークを介した商取引や重要な情報の授受に必要とされる安全性を提供することは難しい。

一方、本人を証明する情報として、パスワードの代わりに生体情報を用いた遠隔本人認証システムを導入すれば、ネットワークを介して重要な情報を安全に授受することが可能である。

【００２２】

例えば、図１８に示すように、認証サーバ装置４２０は、指紋データ測定装置４３０によって得られた指紋データを暗号化部４１４によって暗号化し、得られた暗号化指紋データをパスワードの代わりに通信制御部４１３を介してネットワークに送出する構成とすればよい。

この場合に、認証サーバ装置４２０に備えられた認証制御部４０１は、通信制

御部４２２を介して受け取った暗号化指紋データを復号化部４２１によって復号化し、復元された指紋データをユーザＩＤとともに指紋照合装置４４０の処理に供する構成とすればよい。

【００２３】

更に、生体情報が揺らぎやノイズを含んでいることを前提とし、以前に入力された生体情報と全く同一の生体情報が認証情報として入力されたときに、その生体情報は盗まれたものと判断すれば、盗まれた生体情報を使った侵入（リプレイアタック）を阻止することが可能となり、より一層安全に情報の授受を行うことができる。

【００２４】

例えば、図１８に示した指紋データベース４４１に、各ユーザＩＤに対応する標準データとともに、該当するユーザＩＤについて過去に入力された指紋データを蓄積しておき、照合判定部４４４に備えられた比較部４４５により、入力された指紋データと上述した標準データおよび過去の指紋データとを比較し、この比較結果を不正検出部４４６および照合結果判定部４４７の処理に供する構成とすればよい。

【００２５】

図１８に示した不正検出部４４６は、比較部４４７から受け取った比較結果に基づいて、入力された指紋データを構成する全ての数値データと標準データあるいは過去の指紋データの該当する数値データとが数値として完全に一致しているか否かを判定し、一致していた場合にリプレイアタックを検出した旨を照合結果判定部４４７に通知する構成となっている。

【００２６】

一方、照合結果判定部４４７は、比較部４４７から受け取った比較結果に基づいて、入力された指紋データと標準データとの差が所定の誤差範囲内に収まっているか否かを判定し、この判定結果と上述した不正検出部４４６による検出結果とに応じて、入力された指紋データが本人のものであるか否かを判定し、この判定結果を照合結果として認証制御部４０１に通知する構成となっている。

【００２７】

この場合は、入力された指紋データが、例えば、図１７(ａ)に示した注目範囲を含む範囲に渡って標準データと所定の誤差範囲内で一致しており、かつ、入力された指紋データを構成する全ての数値データが標準データあるいは過去の指紋データに含まれる該当する数値データと数値として完全に同一ではないことが、本人であると認証するための条件となる。

【００２８】

ところで、上述したＤＥＳ方式に代表される従来の暗号化技術は、暗号化された情報から元の情報を復元する際の困難さを重要視しており、複雑な暗号化アルゴリズムによって元の情報を変換しているので、暗号化された生体情報を解読して、元の生体情報を得ることは非常に困難である。

また、生体情報それ自体は、利用者それぞれに固有のものであるから、適切に管理されていれば、これを盗んだり、偽造することもまた非常に困難である。

【００２９】

しかし、暗号化された生体情報（以下、暗号化生体情報と称する）がネットワークを介して伝送される過程はほとんど無防備であるため、暗号化生体情報を不正取得することは比較的容易である。

もちろん、盗聴などの方法によって不正に取得された暗号化生体情報がそのまま利用された場合は、上述したようにして、リプレイアタックとして排除することが可能である。

【００３０】

しかしながら、不正取得された暗号化生体情報の一部が改竄された場合には、この改竄が復号化後の生体情報に及ぼす影響によって、本人であると認証するための条件を満たしてしまう可能性がある。

なぜなら、上述した暗号化部４１４によって、ＤＥＳ方式などのブロック暗号化方式を用いて暗号化された指紋データは、復号化部４２１によって、暗号化の際と同様のブロックごとに復号されるため、暗号化生体情報の改竄は、改竄された部分を復号して得られた部分に局所的に影響するだけで、復号結果の該当する個所以外に波及しないからである。

【００３１】

したがって、例えば、図１９に示すように、ネットワークにおいて暗号化された指紋データ（以下、暗号化指紋データとして示す）を不正取得し、この暗号化指紋データの一部（図１９において斜線を付して示す）を改竄して、新たな認証情報として入力することによって、復号化後の指紋データに擬似的な揺らぎを合成することが可能である。

【００３２】

例えば、図１９に示したように、照合処理に利用されていない部分に対応する暗号化指紋データが改竄された場合に、復号化部によって得られる指紋データは、改竄された箇所に対応する部分が元の指紋データと異なっているものの、注目範囲については元の指紋データと同一である。

このように、改竄された暗号化指紋データを復号化して、元の指紋データとは注目範囲以外の部分で異なっている復号結果（以下、疑似指紋データと称する）が得られた場合に、この疑似指紋データと標準データとは、注目範囲に渡って許容される誤差の範囲内で一致し、かつ、この疑似指紋データは標準データおよび過去に入力された指紋データのいずれとも完全には一致しない。

【００３３】

このような場合に、暗号化指紋データの改竄によって生じた元の指紋データとの差異が、指紋データの揺らぎと判定されてしまう可能性があり、このために、改竄された暗号化指紋データを用いた不正な侵入をリプレイアタックとして排除することができない場合が生じてしまう。

したがって、従来の暗号化技術を単純に利用したのでは、生体情報をネットワークを介して送受信して個人認証処理に供するシステムにおいて、生体情報を利用したことによって期待されるセキュリティの向上を得ることができない。

【００３４】

本発明は、本人を証明するための認証情報を安全かつ確実に伝達するための暗号化・復号化方法および装置並びに、生体情報の特徴を利用した遠隔本人認証システムを提供することを目的とする。

【００３５】

【課題を解決するための手段】

図１に、請求項１および請求項２の発明の原理を示す。

〔００３６〕

請求項１の発明は、図１(ａ)に示すように、個人に固有の特徴を表す生体情報の入力を受け（Ｓ１１）、暗号化の都度、任意の値を持つ数値キーを決定し（Ｓ１２）、数値キーと所定の一次鍵とから暗号鍵を生成し（Ｓ１３）、暗号鍵を用いて生体情報を暗号化し（Ｓ１４）、得られた暗号化生体情報と数値キーとに基づいて、復号化処理側で暗号鍵を再生するための復号制御情報を作成し（Ｓ１５）、暗号化生体情報と復号制御情報とを組み合わせて認証情報を作成する（Ｓ１６）ことを特徴とする。

〔００３７〕

請求項１の発明は、暗号化生体情報を用いて、暗号鍵の生成に用いられた数値キーを示す復号制御情報を作成することにより、復号制御情報と暗号化生体情報との間に依存関係を形成し、この復号制御情報を復号化側による暗号鍵復元処理に供することにより、暗号化生体情報と復号化側で用いられる暗号鍵との間に依存関係を形成することができる。

〔００３８〕

請求項２の発明は、図１(ｂ)に示すように、暗号化生体情報と復号制御情報との組み合わせを受け取り（Ｓ２１）、暗号化生体情報と復号制御情報とに基づいて、暗号化処理側において暗号鍵の生成に用いられた数値キーを復元し（Ｓ２２）、数値キーと所定の一次鍵とに基づいて、暗号化処理側において用いられた暗号鍵を復元し（Ｓ２３）、暗号鍵を用いて暗号化生体情報を復号化し、生体情報を復元する（Ｓ２４）ことを特徴とする。

〔００３９〕

請求項２の発明は、受け取った復号制御情報と暗号化生体情報とに基づいて、まず、数値キーを復元し、この数値キーと一次鍵とから暗号化側で用いられた暗号鍵を復元することにより、請求項１の暗号化方法を用いて得られた暗号化生体情報を暗号化生体情報に依存した暗号鍵を用いて復号し、元の生体情報を復元することができる。

〔００４０〕

図２に、請求項３の暗号化装置及び請求項４の復号化装置の原理ブロック図を示す。

請求項３の発明は、図２(ａ)に示すように、個人に固有の特徴を表す生体情報を入力する生体情報入力手段１１１と、生体情報を暗号化する度に、任意の値を持つ数値キーを決定する数値キー決定手段１１２と、数値キーと所定の一次鍵とに基づいて暗号鍵を生成する暗号鍵生成手段１１３と、暗号鍵を用いて、入力された生体情報を暗号化する第１暗号化手段１１４と、第１暗号化手段１１４によって得られた暗号化生体情報と数値キーとに基づいて、復号化処理側で暗号鍵を再生するために用いる復号制御情報を作成する制御情報作成手段１１５と、暗号化生体情報と復号制御情報とを組み合わせた認証情報を作成する作成手段１１６とを備えたことを特徴とする。

【００４１】

請求項３の発明は、数値キー決定手段１１２、暗号鍵生成手段１１３および第１暗号化手段１１４の動作により、生体情報入力手段１１１を介して入力された生体情報を使い捨ての暗号鍵を用いて暗号化するとともに、制御情報作成手段１１５により、暗号化された生体情報と上述した数値キーとに基づいて復号制御情報を作成することにより、復号制御情報と暗号化生体情報との間に依存関係を形成し、復号化側で用いる暗号鍵と暗号化生体情報との間に依存関係を形成することができる。

【００４２】

したがって、作成手段１１６によって作成された認証情報をそのまま復号処理に供する限りにおいて元の生体情報への復元を保証するとともに、暗号化生体情報あるいは復号制御情報の改竄に応じて暗号鍵の復元を不可能とし、元の生体情報への復元を阻止することができる。

請求項４の発明は、図２(ｂ)に示すように、生体情報を所定の暗号化方法に従って暗号化して得られる暗号化生体情報と復号処理に用いる復号制御情報とを含む認証情報を受け取る受取手段１１７と、認証情報に含まれる暗号化生体情報と復号制御情報とに基づいて、暗号化鍵の生成に用いられた数値キーを作成する数値キー復元手段１１８と、数値キーと所定の一次鍵とに基づいて、暗号鍵を生成

する暗号鍵生成手段１１３と、暗号鍵を用いて暗号化生体情報を復号化する第１復号化手段１１９とを備えたことを特徴とする。

【００４３】

請求項４の発明は、受取手段１１７を介して受け取った暗号化生体情報と復号制御情報とに基づいて、数値キー復元手段１１８と暗号鍵生成手段１１３とが動作することにより、暗号化生体情報と復号制御情報との依存関係を利用して、暗号化側で用いられた暗号鍵を復元し、第１復号化手段１１９の処理に供することができる。

【００４４】

請求項５の発明は、個人に固有の特徴を表す生体情報を入力する生体情報入力手順と、生体情報を暗号化する度に、無作為に任意の数値キーを決定する数値キー決定手順と、数値キーと所定の一次鍵とに基づいて暗号鍵を生成する暗号鍵生成手順と、暗号鍵を用いて、入力された生体情報を暗号化する第１暗号化手順と、第１暗号化手順において得られた暗号化生体情報と数値キーとに基づいて、復号化処理側で暗号鍵を再生するために用いる復号制御情報を作成する制御情報作成手順と、暗号化生体情報と復号制御情報とを組み合わせた認証情報を作成する作成手順とをコンピュータに実行させるプログラムを記録した記憶媒体である。

【００４５】

請求項５の発明は、数値キー決定手順、暗号鍵生成手順および第１暗号化手順を実行して、生体情報入力手順において入力された生体情報を使い捨ての暗号鍵を用いて暗号化するとともに、制御情報作成手順において、暗号化された生体情報と上述した数値キーとに基づいて復号制御情報を作成することにより、復号制御情報と暗号化生体情報との間に依存関係を形成することができる。

【００４６】

したがって、作成手順において作成された暗号化生体情報と復号制御情報との組み合わせをそのまま復号処理に供する限りにおいて元の生体情報への復元を保証するとともに、暗号化生体情報あるいは復号制御情報の改竄に応じて、元の生体情報への復元を阻止することができる。

請求項６の発明は、生体情報を所定の暗号化方法に従って暗号化して得られる

暗号化生体情報と復号処理に用いる復号制御情報とを含む認証情報を受け取る受取手順と、認証情報に含まれる暗号化生体情報と復号制御情報とに基づいて、暗号化鍵の生成に用いられた数値キーを作成する数値キー復元手順と、数値キーと所定の一次鍵とに基づいて、暗号鍵を生成する暗号鍵生成手順と、暗号鍵を用いて暗号化生体情報を復号化する第１復号化手順とをコンピュータに実行させるプログラムを記録した記憶媒体である。

【００４７】

請求項６の発明は、受取手順において受け取った暗号化生体情報と復号制御情報とに基づいて、数値キー復元手順と暗号鍵生成手順とを実行することにより、暗号化生体情報と復号制御情報との依存関係を利用して、暗号化側で用いられた暗号鍵を復元し、第１復号化手順の処理に供することができる。

図３に、請求項７及び請求項８の発明の原理を示す。

【００４８】

請求項７の発明は、図３（ａ）に示すように、個人に固有の特徴を表す生体情報の入力を受け（Ｓ３１）、生体情報を構成する各要素について、その前後を含む所定の範囲に含まれる複数の要素を引数とする所定の関数を用いて数値変換することによって、生体情報をスクランブルし（Ｓ３２）、スクランブルされた生体情報を所定の暗号鍵を用いて暗号化する（Ｓ３３）ことを特徴とする。

【００４９】

請求項７の発明は、暗号化操作に先立って、入力された生体情報を所定の関数を用いてスクランブルすることにより、元の生体情報を構成する各単位情報（以下、ブロックと称する）およびこのブロックと所定の関係を持つ複数のブロックとを反映したスクランブル結果を暗号化操作の対象とすることができる。

このようにして、生体情報を構成する各ブロックに対応する暗号化結果に、このブロックと所定の関係を持つ複数のブロックの内容を反映することにより、暗号化処理における処理単位の長さにかかわらず、暗号化生体情報の各ブロックと、生体情報を構成している複数のブロックとの間に依存関係を形成することができる。

【００５０】

請求項８の発明は、図３（ｂ）に示すように、暗号化生体情報を受け取り（Ｓ４１）、暗号化生体情報を所定の暗号鍵を用いて復号化し（Ｓ４２）、復号結果に含まれる各要素に含まれる元の複数の要素の寄与分を分離してスクランブルを解除し、生体情報を復元する（Ｓ４３）ことを特徴とする。

請求項８の発明は、暗号化側から送出された暗号化生体情報をそのまま受け取った場合には、復号化操作の後に、所定の関数を用いて数値変換することにより、スクランブルを解除して元の生体情報を復元することができる。

【００５１】

一方、暗号化生体情報に改竄が加えられていた場合には、改竄箇所に対応する復号結果のブロックの内容が変化したことにより、このブロックと依存関係を持つ複数のブロックに渡ってスクランブル解除結果が変化するため、復号化処理における処理単位の長さにかかわらず、元の生体情報を復元することができない。

図４に、請求項９の暗号化装置及び請求項１０の復号化装置の原理ブロック図を示す。

【００５２】

請求項９の発明は、図４（ａ）に示すように、個人に固有の特徴を表す生体情報を入力する生体情報入力手段１１１と、生体情報の入力に応じて、生体情報を構成する各要素を含む複数の要素を引数とする所定の関数を用いて数値変換するスクランブル手段１３１と、スクランブル手段１３１による変換結果を所定の暗号鍵を用いて暗号化する第２暗号化手段１３２とを備えたことを特徴とする。

【００５３】

請求項９の発明は、スクランブル手段１３１および第２暗号化手段１３２の動作により、生体情報入力手段１１１によって入力された生体情報を構成する各ブロックに含まれる情報とそのブロックと所定の関係を持つ複数のブロックに含まれる情報とを、生体情報の各ブロックに対応する暗号化生体情報の各ブロックに反映することができる。

【００５４】

すなわち、暗号化生体情報を構成する各ブロックは、生体情報を構成している複数のブロックに含まれる情報に依存しているから、この暗号化生体情報をその

まま復号処理に供する限りにおいて元の生体情報への復元を保証するとともに、暗号化生体情報が一部でも改竄された場合には、元の生体情報への復元を阻止することができる。

【００５５】

請求項１０の発明は、図４（ｂ）に示すように、生体情報をスクランブルした後に暗号化して得られる暗号化生体情報を受け取って、所定の暗号鍵を用いて復号化する第２復号化手段１３５と、復号結果を所定の関数を用いて数値変換することによって、暗号化処理において施されたスクランブルを解除するスクランブル解除手段１３６とを備えたことを特徴とする。

【００５６】

請求項１０の発明は、暗号化側から送出された暗号化生体情報をそのまま受け取った場合には、第２復号手段１３５およびスクランブル解除手段１３６の動作により、復号結果に施されたスクランブルを解除して元の生体情報を復元することができる。

一方、暗号化生体情報に改竄が加えられていた場合には、改竄箇所に対応する復号結果のブロックの内容が変化したことにより、このブロックと依存関係を持つ複数のブロックに渡ってスクランブル解除結果が変化するため、元の生体情報を復元することができない。

【００５７】

請求項１１の発明は、個人に固有の特徴を表す生体情報を入力する生体情報入力手順と、生体情報を暗号化する度に、生体情報を構成する各要素を含む複数の要素を引数とする所定の関数を用いて数値変換するスクランブル手順と、スクランブル手順による変換結果を所定の暗号鍵を用いて暗号化する第２暗号化手順とをコンピュータに実行させるプログラムを記録した記憶媒体である。

【００５８】

請求項１１の発明は、スクランブル手順および第２暗号化手順を実行することにより、生体情報入力手順において入力された生体情報を構成する各ブロックに含まれる情報とそのブロックと所定の関係を持つ複数のブロックに含まれる情報とを、生体情報の各ブロックに対応する暗号化生体情報の各ブロックに反映する

ことができる。

【００５９】

この場合は、暗号化生体情報を構成する各ブロックは、生体情報を構成している複数のブロックに含まれる情報に依存しているから、この暗号化生体情報をそのまま復号処理に供する限りにおいて元の生体情報への復元を保証するとともに、暗号化生体情報が一部でも改竄された場合には、元の生体情報への復元を阻止することができる。

【００６０】

請求項１２の発明は、生体情報をスクランブルした後に暗号化して得られる暗号化生体情報を受け取って、所定の暗号鍵を用いて復号化する第２復号化手順と、復号結果を所定の関数を用いて数値変換することによって、暗号化処理において施されたスクランブルを解除するスクランブル解除手順とをコンピュータに実行させるプログラムを記録した記憶媒体である。

【００６１】

請求項１２の発明は、暗号化側から送出された暗号化生体情報をそのまま受け取った場合には、第２復号手順およびスクランブル解除手順を実行することにより、復号結果に施されたスクランブルを解除して元の生体情報を復元することができる。

一方、暗号化生体情報に改竄が加えられていた場合には、改竄箇所に対応する復号結果のブロックの内容が変化したことにより、このブロックと依存関係を持つ複数のブロックに渡ってスクランブル解除結果が変化するため、元の生体情報を復元することができない。

【００６２】

図５に、請求項１３の遠隔本人認証システムの原理ブロック図を示す。

請求項１３の発明は、認証クライアント装置１０１と認証サーバ装置１０２とがネットワークを含む伝送媒体を介して暗号化した認証情報を授受して、本人認証処理に供する遠隔本人認証システムにおいて、認証クライアント装置１０１は、個人に固有の特徴を表す生体情報を入力する生体情報入力手段１１１と、利用者が自身の資格を証明するための資格情報として、他者に公開されている識別情

報と他者からは秘匿されるべきパスワードとを含む情報を入力する資格情報入力手段１４１と、パスワードを暗号鍵として、生体情報を暗号化する第３暗号化手段１４２と、第３暗号化手段１４２によって得られた暗号化生体情報と識別情報との組み合わせを認証情報として前記伝送媒体に送出する出力手段１４３とを備えた構成であり、認証サーバ装置１０２は、全ての利用者に対応する識別情報に対応して、パスワードと該当する個人の生体的な特徴を計測して得られた標準情報とを登録する資格情報登録手段１４４と、前記伝送媒体を介して、暗号化生体情報と識別情報との組み合わせを受け取る入力手段１４５と、入力手段１４５を介して受け取った識別情報に基づいて、資格情報登録手段１４４から該当するパスワードおよび標準情報を検索する検索手段１４６と、検索手段１４６を介して受け取ったパスワードを暗号鍵として、入力手段から受け取った暗号化生体情報を復号化する第３復号化手段１４７と、第３復号化手段１４７によって復元された生体情報と検索手段１４６によって検索された標準情報とを照合する照合手段１４８とを備えた構成であることを特徴とする。

【００６３】

請求項１３の発明は、認証クライアント装置１０１において、資格情報入力手段１４１を介して入力された資格情報を暗号鍵として、第３暗号化手段１４２が動作することにより、生体情報入力手段１１１を介して入力された生体情報が揺らぎ情報を含んでいることを利用して、認証処理の都度に異なるビットパターンで表される暗号化生体情報を含む認証情報を生成し、出力手段１４３を介して伝送媒体に送出することができる。

【００６４】

この認証情報が伝送媒体を介してそのまま認証サーバ装置１０２に備えられた入力手段１４５に伝達された場合は、検索手段１４６および第３復号化手段１４７が動作することにより、認証クライアント装置１０１側で入力された生体情報が復元されるので、照合手段１４８により、生体情報の揺らぎを考慮して、この復元された生体情報と資格情報登録手段１４４に登録された標準情報とを照合することにより、確実に本人を確認することができる。

【００６５】

これにより、使い捨ての暗号鍵を用いてパスワードを暗号化した場合と同様に、安全にパスワードを授受することが可能となり、遠隔本人認証システムの安全性を向上することができる。

【００６６】

【発明の実施の形態】

以下、図面に基づいて、本発明の実施形態について詳細に説明する。

【００６７】

図６に、請求項３の暗号化装置および請求項４の復号化装置を適用した遠隔本人認証システムの構成を示す。また、図７に、暗号化装置による暗号化動作および復号化装置による復号化動作を表す流れ図を示す。

図６に示した認証クライアント装置２０１において、暗号化装置２１０は、指紋データ測定装置４３０（図１６参照）によって得られた指紋データを暗号化し、得られた暗号化生体情報を通信制御部４１３を介してネットワークに送出する構成となっている。

【００６８】

また、認証サーバ装置２０２において、復号化装置２２０は、通信制御部４２２を介して受け取った暗号化生体情報を復号化して元の指紋データを復元し、指紋照合装置４４０の処理に供する構成となっている。

図６に示した暗号化装置２１０において、ビットパターン作成部２１１は、入力された指紋データを表す一連の数値データに基づいて、所定の長さの巡回冗長検査（ＣＲＣ）パターンを作成し（図７(ａ)において、ステップ３０１、３０２に示す）、数値キーとして暗号鍵生成部２１２の処理に供する構成となっている。

【００６９】

ここで、上述した指紋データ測定装置４３０によって得られた指紋データは、測定対象の人物に固有の特徴を表す固有情報とともに、測定条件などによって変動する揺らぎ情報を含んでいる。

したがって、上述したビットパターン作成部２１１により、この揺らぎ情報を表すビット列に基づいて、ｎビットのＣＲＣパターンを作成すれば、必ず、指紋

データの入力ごとに異なるビットパターンが得られ、暗号化の都度に変化する数値キーとして利用することが可能である。

【００７０】

すなわち、このように、ビットパターン作成部２１１が動作して、得られたビットパターン数値キーを暗号鍵生成部２１２に渡すことにより、後述する追加開示項１で述べる揺らぎ抽出手段１２１および数値変換手段１２２の機能を実現し、指紋データの揺らぎを利用して、ランダムな数値データを作成することができるので、この場合は、このビットパターン作成部２１１により、請求項３で述べた数値キー決定手段１１２の機能が果たされている。

【００７１】

また、図６において、一次鍵保持部２１３は、一次鍵として、長さｎビットのビットパターンを保持しており、暗号鍵生成部２１２は、例えば、この一次鍵とビット列とについて排他的論理和演算を行うことによって、請求項３で述べた暗号鍵生成手段１１３の機能を実現してｎビットの暗号鍵を生成し（図７(ａ)のステップ３０３）、第１暗号化手段１１４に相当するブロック暗号化部２１４の処理に供する構成となっている。

【００７２】

例えば、認証クライアント装置２０１を識別するための装置パスワードが予め登録されている場合は、この装置パスワードまたはその一部を一次鍵として、一次鍵保持部２１３に保持すればよい。また、利用者が入力するユーザパスワードを一次鍵として利用することも可能であるし、更に、装置パスワードとユーザパスワードとを組み合わせて得られたビットパターンを一次鍵として、一次鍵保持部２１３に保持しておいてもよい。

【００７３】

一般に、暗号鍵が長いほど暗号化情報の解析が困難になるので、３２ビット以上のビットパターンを暗号鍵として生成すべきである。

特に、ビットパターン生成部２１１により５６ビットのＣＲＣパターンを作成するとともに、一次鍵として同じ長さのビットパターンを保持しておき、暗号鍵生成部２１２により、５６ビットの暗号鍵を生成すれば、ＤＥＳ方式などのブロ

ック暗号化技術を適用することができる。

【００７４】

この場合は、ブロック暗号化部２１４は、例えば、ＤＥＳ方式に従って、上述した暗号鍵を用いて暗号化し（図７(ａ)のステップ３０４）、得られた暗号化指紋データをハッシュ変換部２１５と認証情報結合部２１６との処理に供する構成とすればよい。

このハッシュ変換部２１５は、適切なハッシュ関数を用いて、例えば、暗号化指紋データをそれ自身の長さよりも短いビット列で表されるハッシュアドレスに変換する構成となっている。

【００７５】

また、このハッシュ変換部２１５によって得られたハッシュアドレスは、上述した数値キーとともに論理演算部２１７に入力されており、この論理演算部２１７は、ハッシュアドレスと数値キーとの組み合わせを１対１写像関数によって変換する操作を示す所定の論理演算を行って、演算結果を認証情報結合部２１５に渡す構成となっている。

【００７６】

ここで、上述したハッシュ変換部２１５において、十分な拡散性を備えたハッシュ関数を用いれば、暗号化指紋データの入力に応じてハッシュ変換部２１５が動作することにより（図７(ａ)のステップ３０５）、後述する追加開示項２で述べる要約手段１２３の機能を実現し、暗号化指紋データの概略を反映する要約情報に相当する情報を得ることができる。

【００７７】

また、ハッシュアドレスと数値キーの入力に応じて、論理演算部２１７が、例えば、これらの排他的論理和を算出することにより（図７(ａ)のステップ３０６）、２つの入力の組み合わせに１対１で対応する写像に変換することができるから、後述する追加開示項２で述べる合成手段１２４の機能を実現し、ハッシュアドレスと数値キーとの双方を反映した論理演算結果を得ることができる。

【００７８】

この場合は、上述したハッシュ変換部２１５と論理演算部２１７とにより、請

求項３で述べた制御情報作成手段１１５の機能が果たされており、簡単な演算処理によって、暗号化指紋データに対応する要約情報と数値キーとの双方を反映した復号制御情報を得ることが可能である。

このようにして、復号制御情報と暗号化指紋データとの間に依存関係を形成したことにより、後述するように、復号化装置において利用する暗号鍵は、復号制御情報および暗号化指紋データの双方に依存して変化するから、ネットワークを介して伝送される暗号電文の改竄に応じて、暗号鍵の復元を不可能にすることができる。

【００７９】

一方、図６に示した認証情報結合部２１６は、例えば、ブロック暗号化部２１４から受け取った暗号化指紋データと上述した復号制御情報とを単純に結合し（図７(ａ)のステップ３０７）、図８に示すような一連のビット列で表される認証情報を作成し、通信制御部４１３を介してネットワークに送出する構成となっている。

【００８０】

このように、暗号化指紋データおよび復号制御情報の入力に応じて、認証情報結合部２１６が動作することにより、後述する追加開示項３で述べる作成手段１１６の機能を実現し、暗号化指紋データと復号制御情報とを一体化して、通信制御部４１３を介してネットワークに送出することができる。

このようにして、図６に示した暗号化装置２１０の各部が動作することにより、請求項１の暗号化方法を用いて指紋データを暗号化し、ネットワークを介して認証サーバ装置２０２に備えられた復号化装置２２０による復号化処理に供することができる。

【００８１】

図６に示した復号化装置２２０において、制御情報分離部２２２は、通信制御部４２２を介して図８に示したような認証情報を受け取り（図７(ｂ)のステップ３１１）、この認証情報を暗号化指紋データと復号制御情報とに分離して（図７(ｂ)のステップ３１２）、暗号化指紋データを復号化部２２３およびハッシュ変換部２２４に送出するとともに、復号制御情報を論理演算部２２５に送出する構

成となっている。

〔００８２〕

このように、認証情報の入力に応じて、制御情報分離部２２２が動作することにより、請求項４で述べた受取手段１１７の機能が果たされている。

ここで、上述したように、復号制御情報は、暗号化指紋データに対応するハッシュアドレスと数値キーとの排他的論理和演算結果である。

したがって、ハッシュ変換部２２４により、暗号化側と同一のハッシュ関数を用いて暗号化指紋データのハッシュアドレスを求め（図７(ｂ)のステップ３１３）、論理演算部２２５により、このハッシュアドレスと復号制御情報との排他的論理和を求めることにより（図７(ｂ)のステップ３１４）、請求項４で述べた数値キー復元手段１１８の機能を実現し、暗号鍵を作成する際に用いられた数値キーを復元することができる。

〔００８３〕

このとき、ハッシュ変換部２２４および論理演算部２２５は、後述する追加開示項４で述べる要約手段１２３および分離手段１２５の機能をそれぞれ果たしている。

また、図６において、一次鍵保持部２２６は、暗号化側で用いられた一次鍵を保持しており、一次鍵保持部２２６および暗号鍵生成部２２７が、論理演算部２２５による演算結果を数値キーとして受け取って動作することにより（図７(ｂ)のステップ３１５、３１６）、暗号鍵生成手段１１３の機能を果たし、暗号化側で用いられた暗号鍵を再生して、ブロック復号化部２２３の処理に供することができる。

〔００８４〕

このように、復号制御情報と暗号化指紋データとに基づいて、ハッシュ変換部２２４および論理演算部２２５により、暗号化に用いられた数値キーを復元し、暗号鍵生成部２２７を介してブロック復号化部２２３の処理に供する構成とすることにより、請求項２で述べた復号化方法に従って復号化処理を行う復号化装置を実現し、上述した暗号化装置２１０による暗号化指紋データを含んだ認証情報から元の指紋データを復元することができる。

【００８５】

次に、ネットワークを伝搬する過程で認証情報の一部が改竄された場合に、上述した構成の復号化装置２２０を備えた認証サーバ装置１０２が、不正なアクセスを排除する方法について説明する。

例えば、図８(ａ)に示すように、認証情報に含まれる暗号化指紋データの一部（図８において、網掛けを付して示す）が改竄された場合は、この暗号化指紋データの入力に応じて、ハッシュ変換部２２４によって得られるハッシュアドレスは、当然ながら、元の暗号化指紋データをハッシュ変換して得られるハッシュアドレスとは異なっている。

【００８６】

この場合は、暗号化指紋データの改竄によって誤った要約情報が得られるので、この誤った要約情報と復号制御情報とを論理演算部に入力して得られる数値キーもまた誤った数値キーとなり、更には、暗号鍵生成部を介して暗号鍵にも誤りが伝搬する。

これにより、ブロック復号化部２２３は、改竄された暗号化指紋データを誤った暗号鍵を用いて復号化することになるので、復号結果は、元の指紋データとは大きく異なっていると期待できる。

【００８７】

また、図８(ｂ)に示すように、認証情報に含まれる復号制御情報が改竄されていた場合は、暗号化指紋データの入力に応じて、ハッシュ変換部２２４によって正しいハッシュアドレスが得られるものの、復号制御情報が誤っているために、論理演算部による演算結果は元の数値キーとは異なる誤った数値キーとなる。

この場合も、暗号化指紋データが改竄された場合と同様に、誤った暗号鍵が復号化部の処理に供されるので、復号化部によって得られる復号結果もまた、元の指紋データとは大きく異なっていると期待できる。

【００８８】

このように、請求項１の暗号化方法および請求項２の復号化方法を適用すれば、暗号化された認証情報の一部が改竄され、暗号化側で形成された暗号化生体情報と復号制御情報との間の依存関係が破壊されたときに、この改竄の影響を復号

結果全体に波及させることができる。

上述したように、誤った暗号鍵を用いて得られた復号結果と元の指紋データとの違いは甚だしいと考えられるから、改竄された認証情報の入力に応じて得られた指紋データは、指紋照合装置４４０によって、確実に本人のものではないと判断することが可能である。

【００８９】

なぜなら、図８に示したように、認証情報の任意の部分が改竄された影響は、復号結果全体におよんでいるので、指紋照合装置４４０における注目範囲も確実に無視できない影響を受けると期待できるからである。

【００９０】

したがって、照合処理にかかわる注目範囲の長さにかかわらず、改竄された認証情報から復元された指紋データは、指紋照合装置４４０により、確実に本人のものではないと判定されるので、不正取得した暗号化生体情報に基づくアクセスを確実に排除することが可能である。

また、図１８に示した指紋照合部４４０のように、標準データあるいは過去に入力された指紋データと同一の指紋データが入力されたときに、リプレイアタックとして排除する構成を採用すれば、不正に取得した認証情報をそのまま利用したアクセスも排除することができる。

【００９１】

このように、請求項３の暗号化装置と請求項４の復号化装置を組み合わせることにより、生体情報に含まれている固有情報と揺らぎ情報との特徴をそれぞれ利用して、本人を確実に認証することが可能となり、安全性の高い遠隔本人認証システムを提供することができる。

なお、暗号化部２１４において採用する暗号化方法は、共通鍵方式の暗号化方法であればよいので、上述したＤＥＳ方式の代わりに、アフィン暗号やビジュネール暗号などを採用してもよい。

【００９２】

また、暗号化部２１４による暗号化処理の単位の長さを変更することも可能である。

例えば、暗号化単位の長さを３２ビットとするとともに、一次鍵および数値キーをともに３２ビットとして、暗号鍵生成部２１３により３２ビットの暗号鍵を生成し、暗号化部２１４では、この暗号鍵を乱数系列種として各ブロックについて順次に乱数を求め、この乱数と該当するブロックとの排他的論理和演算の結果を暗号化データとする構成としてもよい。

【００９３】

また、暗号化生体情報の要約情報は、暗号化生体情報全体に依存していればよいので、例えば、ハッシュ変換部２１５、２２４の代わりに、暗号化生体情報を表すビット列から単純にビットを間引いて要約情報を作成する間引き処理部を備えて暗号化装置および復号化装置を構成してもよいし、暗号化生体情報についてのＣＲＣパターンを要約情報として作成するＣＲＣパターン作成部を備えて暗号化装置および復号化装置を構成することもできる。

【００９４】

また、図６に示した通信制御部４１３に代えてＩＣカードライタを備えて認証クライアント装置２０１を構成するとともに、通信制御部４２２に代えてＩＣカードリーダを備えて認証サーバ装置２０２を構成し、ＩＣカードを介して認証情報を授受する構成としてもよい。

この場合は、例えば、ＩＣカードを備えたネームプレートを利用者が携帯することにより、認証情報を認証サーバ装置に渡すことができる。

【００９５】

また、図６に示した暗号化装置２１０を構成する各部の機能は、請求項５で述べた生体情報入力手順、数値キー作成手順、暗号鍵作成手順、第１暗号化手順および制御情報作成手順をコンピュータに実行させるプログラムによって実現可能であり、このプログラムを記憶媒体に記録して頒布することにより、請求項１で述べた暗号化方法を用いて生体情報を安全に暗号化するシステムを幅広い利用者に提供することができる。

【００９６】

同様に、図６に示した復号化装置２２０を構成する各部の機能は、請求項６で述べた数値キー復元手順、暗号鍵作成手順および第１復号手順をコンピュータに

実行させるプログラムによって実現可能であり、このプログラムを記憶媒体に記録して頒布することにより、請求項１で述べた暗号化方法を用いて暗号化された正当な認証情報のみを正しく復号して生体情報を復元し、照合処理に供するシステムを提供することができる。

【００９７】

次に、請求項７から請求項１２の発明について説明する。

図９に、請求項９の暗号化装置および請求項１０の復号化装置を適用した本人認証システムの構成を示す。

【００９８】

図９に示した本人認証システムにおいて、認証クライアント装置２０３に備えられた暗号化装置２３０は、指紋データ測定装置４３０から受け取った指紋データを暗号化し、得られた暗号化指紋データを認証情報としてＩＣカードライタ２３４を介してＩＣカードに書き込む構成となっている。

また、図９に示した認証サーバ装置２０４に備えられた復号化装置２４０は、ＩＣカードに書き込まれた認証情報をＩＣカードリーダ２３５を介して受け取って復号化し、復元した指紋データを指紋照合装置４４０の処理に供する構成となっている。

【００９９】

図９に示した暗号化装置２３０において、離散フーリエ変換（ＤＦＴ）演算部２３１は、請求項９で述べたスクランブル手段１３１に相当するものであり、指紋データ測定装置４３０から受け取った指紋データをフーリエ変換し、変換結果をブロック暗号化部２３２の処理に供する構成となっている。

また、図９に示した暗号鍵保持部２３３は、登録された各認証クライアント装置に固有の暗号鍵を保持しており、ブロック暗号化部２３２は、この暗号鍵を用いて、ＤＦＴ演算部２３１による変換結果をブロックごとに暗号化し、ＩＣカードライタ２３４による書込処理に供する構成となっている。

【０１００】

例えば、暗号鍵保持部２３３に５６ビットの暗号鍵を保持し、ブロック暗号化部２３２における暗号化方法としてＤＥＳ方式を採用すれば、非常に解読困難な

暗号化指紋データを得ることができ、これにより、請求項９で述べた第２暗号化手段１３２の機能を果たすことができる。

ここで、ＤＦＴ演算部２３１が指紋データをフーリエ変換することにより、後に追加開示項５において述べるスクランブル手段１３１の機能が果たされ、図１０(ａ)、(ｂ)に示すように、指紋データの各部分の寄与分がフーリエ変換結果の全体に拡散するので、ブロック暗号化部２３２による暗号化処理単位となる各ブロックは、指紋データを構成する全ての情報要素の寄与分を含んでいる（図１０(ｃ)参照）。

【０１０１】

したがって、上述したようにして、指紋データをフーリエ変換した後に暗号化した場合は、暗号化指紋データを構成する各ブロックの情報は、指紋データを構成する全ての情報要素に依存している。

すなわち、上述したように、図９に示した暗号化装置２３０の各部が動作することにより、請求項７で述べた暗号化方法によって生体情報を暗号化し、生体情報を構成する全ての情報要素に依存する部分暗号からなる暗号化生体情報を生成することができる。

【０１０２】

一方、図９に示した復号化装置２４０において、ブロック復号化部２４１は、ＩＣカードリーダ２３５を介して、上述したようにして得られた暗号化指紋データを受け取り、暗号鍵保持部２４２に保持された暗号鍵を用いて、暗号化指紋データを構成する各部分暗号を順次に復号化し、離散フーリエ逆変換（逆ＤＦＴ）演算部２４３の処理に供する構成となっている。

【０１０３】

例えば、上述したように、暗号化側でＤＥＳ方式が採用されている場合は、暗号鍵保持部２４２に暗号化側で用いられた暗号鍵を保持しておき、ブロック復号化部２４１が、ＤＥＳ方式に従って暗号化指紋データの各ブロックを復号化することにより、請求項１０で述べた第２復号化手段１３５の機能を果たすことができる。

【０１０４】

ここで、図１０(ｄ)に示すように、上述した暗号化装置２３０による暗号化指紋データがそのまま復号化装置２４０に到達した場合は、ブロック復号化部２４１の動作により、暗号化装置側のＤＦＴ演算部２３１による変換結果と同一のデータ列が得られる（図１０(ｅ)参照）。

したがって、このブロック復号化部２４１による復号結果の入力に応じて、逆ＤＦＴ演算部２４３が逆フーリエ変換処理を行うことにより、請求項１０で述べたスクランブル解除手段１３６の機能を実現し、スクランブル結果を構成する各情報要素に分散された寄与分を集約してスクランブルを解除し、元の指紋データを復元することができる（図１０(ｆ)参照）。

【０１０５】

このように、請求項７の暗号化方法によって暗号化された暗号化生体情報が、図９に示した復号化装置２４０にそのまま入力された場合には、この復号化装置２４０を構成する各部が上述したようにして動作することにより、請求項８で述べた復号化方法を用いて元の生体情報を完全に復元し、指紋照合装置４４０による照合処理に供することができる。

【０１０６】

一方、図１０(ｇ)に示すように、一部が改竄された暗号化指紋データが入力された場合は、ブロック復号化部２４２および逆ＤＦＴ演算部２４３の動作により、改竄された部分暗号の寄与分がスクランブル解除結果全体に拡散し（図１０(ｈ)、(ｊ)参照）、元の指紋データとは大幅に異なるデータ列となることが期待できる。

このように、暗号化指紋データの改竄に応じて、該当する部分暗号と元の指紋データ全体との依存関係が自動的に破壊されるので、復号化側で元の指紋データを復元するためには、暗号化指紋データを構成する全てのブロックが改竄されないことが必要となり、ネットワーク上において不正に取得された認証情報を改竄して利用する企てを排除することができる。

【０１０７】

また、図９に示した暗号化装置２３０を構成する各部の機能は、請求項１１で述べた生体情報入力手順、スクランブル手順および第２暗号化手順をコンピュー

タに実行させるプログラムによって実現可能であり、このプログラムを記憶媒体に記録して頒布することにより、請求項７で述べた暗号化方法を用いて生体情報を安全に暗号化するシステムを幅広い利用者に提供することができる。

【０１０８】

同様に、図９に示した復号化装置２４０を構成する各部の機能は、請求項１２で述べた第２復号化手順およびスクランブル解除手順をコンピュータに実行させるプログラムによって実現可能であり、このプログラムを記憶媒体に記録して頒布することにより、請求項８で述べた復号化方法を用いて、正当な認証情報のみを正しく復号して生体情報を復元し、照合処理に供するシステムを提供することができる。

【０１０９】

更に、請求項７および請求項８で述べた暗号化方法および復号化方法を適用した場合は、次に述べるように、生体情報の照合処理を解析する企てを阻止する効果と、生体情報そのもののデータ構造を解析する企てを阻止する効果を享受することができる。

まず、図１１を用いて、生体情報照合処理の解析を防ぐ効果を説明する。

【０１１０】

暗号化側でスクランブル処理を行わない場合は、暗号化方法が如何に優れていても、ブロック暗号化方法を採用する限り、暗号化データの改竄による影響は、復号結果の一部におよぶのみである。

したがって、例えば、認証情報の各ブロックを順次に改竄していったときに、その認証情報によるアクセスが受け入れられるか否かを観察することにより、図１１(ａ)に示すように、標準となる生体情報との照合処理において誤差範囲内での一致が必要とされる注目範囲を判別することが可能である。

【０１１１】

一方、スクランブルとブロック暗号化とを組み合わせた場合は、図１１(ｂ)に示すように、復号処理に続いて行われるスクランブル解除処理によって、認証情報を改竄した箇所にかかわらず、スクランブル解除結果全体に改竄の影響が波及するので、注目範囲においても許容される誤差範囲を超える差異が生じ、標準と

なる生体情報との照合結果は必ず不一致となる。

〔０１１２〕

したがって、上述したような方法によって、生体情報を照合する処理を解析することは不可能である。

次に、図１２を用いて、生体情報そのものについてのデータ構造解析を防ぐ効果を説明する。

暗号化側でスクランブル処理を行わない場合は、生体情報を構成する各情報要素の内容の変化は、暗号化データに含まれる該当するブロックの内容に直接に反映される。

〔０１１３〕

したがって、図１２(ａ)に示すように、指紋を表す画像データにおいて、図において円で囲んだ部分を端点から分岐点に改竄したときに、これに応じて暗号化データに現れる変化を監視すれば、指紋を表す画像を構成する部分に関する特徴が指紋データのどこに記述されているかを把握することが可能である。

一方、スクランブルとブロック暗号化とを組み合わせた場合は、図１２(ａ)に示したそれぞれの特徴を指紋データにおいて記述した部分の寄与は、図１２(ｂ)にそれぞれ網掛けの種類を変えて示すように、スクランブル処理の影響により、暗号化データを構成する全てのブロックに渡って分散して現れる。

〔０１１４〕

したがって、上述したような方法により、生体情報のデータ構造を解析することは不可能である。

このように、スクランブルと暗号化とを組み合わせて用いることにより、暗号化生体情報を単純に改竄して試みられた不正アクセスを排除するとともに、生体情報そのものを偽造しようとする企てをも非常に困難にすることができる。

〔０１１５〕

これにより、本人認証システムの安全性を格段に向上することができる。

また、図９に示したＩＣカードライタ２３４に代えて通信制御部を備えて認証クライアント装置２０３を構成するとともに、ＩＣカードリーダ２３５に代えて通信制御部を備えて認証サーバ装置２０４を構成し、ネットワークを介して認証

情報を授受する構成としてもよい。

【０１１６】

ところで、上述したように、指紋データなどの生体情報は、測定条件などに応じて変化する揺らぎ情報を含んでいるために、認識率の向上には限界があり、例えば、図１７において説明したように、注目範囲を狭めた場合には、本人以外の指紋データを本人のものであると誤認識してしまう可能性がある。

一方、パスワードによって本人を確認する手法では、パスワードとユーザＩＤとの組み合わせによって確実に本人を特定することが可能である反面、本人認証システム全体の安全性が、個々の利用者がパスワードを厳密に管理できるか否かにかかっているため、利用者の負担が大きくなってしまっている。

【０１１７】

次に、生体情報の特徴とパスワードの特徴とを組み合わせて、遠隔本人認証システムの安全性を向上する方法について説明する。

図１３に、請求項１３の遠隔本人認証システムの実施形態を示す。

図１３に示した認証クライアント装置１０１において、依頼制御部２５１は、利用者がキーボート４１１を操作して、ユーザＩＤおよびパスワードを入力したときに、このパスワードを暗号鍵としてブロック暗号化部２５２の処理に供するとともに、ユーザＩＤを認証情報作成部２５３に渡す構成となっている。

【０１１８】

この場合は、キーボード４１１によって、請求項１３で述べた資格情報入力手段１４１の機能が果たされており、また、ブロック暗号化部２５２により、第３暗号化手段１４２の機能が果たされている。

このブロック暗号化部２５２は、例えば、ＤＥＳ方式などの共通鍵方式の暗号化方法に従って、依頼制御部２５１から受け取ったパスワードを共通鍵として、指紋データ測定装置４３０から受け取った指紋データを暗号化し、認証情報作成部２５３の処理に供する構成とすればよい。

【０１１９】

また、図１３に示した認証情報作成部２５３は、ブロック暗号化部２５２から受け取った暗号化指紋データと、依頼制御部２５１を介して受け取ったユーザＩ

Ｄとを組み合わせて認証情報を作成し、通信制御部４１３を介してネットワークに送出する構成となっている。

このように、暗号化指紋データおよびユーザＩＤの入力に応じて、認証情報作成部２５３と通信制御部４１３とが動作することにより、請求項１３で述べた出力手段１４３の機能を実現し、暗号化指紋データとユーザＩＤとを含んだ認証情報を出力し、ネットワークを介して認証サーバ装置１０２側に渡すことができる。

【０１２０】

上述したように、指紋データは、利用者固有の特徴を表すものであるが、その特徴を数値化したデータは測定誤差などのために測定の度に変動しているから、この指紋データをパスワードを暗号鍵として暗号化することにより、認証サーバ１０２側に送出される認証情報は、認証依頼の度に異なるビットパターンで表される。

【０１２１】

これにより、パスワードを使い捨ての暗号鍵を用いて暗号化して認証情報とする場合と同様に、ネットワークを介して伝達される認証情報を不正な方法で解読することを非常に困難にすることができる。

一方、図１３に示した認証サーバ装置１０２において、パスワードデータベース２６１は、各ユーザＩＤに対応するパスワードを保持しており、請求項１８で述べた資格情報登録手段１４４の機能の一部を果たしている。

【０１２２】

また、図１３において、パスワード検索部２６２は、請求項１３で述べた検索手段１４６の機能の一部を果たしており、認証制御部４０１からの指示に応じて、パスワードデータベース２６１から該当するパスワードを検索して認証制御部２６３の処理に供する構成となっている。

この認証制御部２６３は、通信制御部４２２を介して上述した認証情報を受け取ることによって請求項１３で述べた入力手段１４５の機能を果たしており、パスワード検索部２６２を介して、この認証情報に含まれているユーザＩＤに対応するパスワードを検索し、得られたパスワードと暗号化指紋データとをブロック

復号化部２６４の処理に供するとともに、ユーザＩＤを指紋照合装置４４０に通知する構成となっている。

【０１２３】

上述したように、暗号化指紋データは、利用者の指紋データを利用者が入力したパスワードを用いて暗号化されているから、請求項１３で述べた第３復号化手段１４７に相当するブロック復号化部２６４は、パスワード検索部２６２によって検索されたパスワードを暗号鍵として復号化処理を行い、復元された指紋データを指紋照合装置４４０の処理に供すればよい。

【０１２４】

図１３において、指紋照合装置４４０に備えられた指紋データベース４４１は、請求項１３で述べた資格情報登録手段１４４の機能の一部を果たしており、ユーザＩＤに対応して該当する利用者の指紋を標準的な条件で測定して得られた標準データを保持している。

また、指紋照合装置４４０に備えられた指紋データ検索部４４２は、上述した認証制御部２６３を介してユーザＩＤを受け取り、指紋データベース４４１から該当する標準データを検索する構成となっている。

【０１２５】

このように、指紋データ検索部４４２が、認証制御部２６３からの指示に応じて動作することにより、請求項１３で述べた検索手段１４６の機能の一部が果たされ、認証情報の一部として入力されたユーザＩＤに対応する標準データが照合判定部４４４による照合処理に供される。

この照合判定部４４４は、ブロック復号化部２６４から受け取った指紋データと上述した標準データとを照合し、照合結果を認証制御部２６３に返す構成となっており、これにより、請求項１３で述べた照合手段１４８の機能が果たされている。

【０１２６】

このようにして、本人の生体情報とパスワードとを組み合わせて利用する遠隔本人認証システムを構成することができる。

この遠隔本人認証システムでは、正当な資格を持つ利用者が、利用者自身の指

紋を指紋データ測定装置４３０による測定に供し、正当なパスワードを入力した場合に限り、上述したブロック復号化部２６４により、指紋データ測定装置４３０によって得られた指紋データが完全に復元され、照合判定部４４４の処理に供される。

【０１２７】

このとき、予め決定された認識率に応じた注目範囲を含む範囲に渡って、復元された指紋データと標準データとが許容される誤差の範囲内で一致するので、指紋照合装置４４０により、標準データと一致した旨の照合結果が得られる。

この場合に、認証制御部２６３は、通信制御部４２２を介して、本人であることを確認した旨の認証結果を認証クライアント装置１０１側に通知し、一方、認証クライアント装置１０１に備えられた依頼制御部２５１は、通信制御部４１３を介してこの認証結果を受け取って、例えば、ＣＲＴディスプレイ装置（ＣＲＴ）４１５を介して、アクセスが認められた旨を利用者に通知すればよい。

【０１２８】

次に、図１３に示した遠隔本人認証システムが、不正アクセスを排除する動作を説明する。

例えば、本人以外の不当な利用者が、正当な資格を持つ利用者から盗んだパスワードを用いてアクセスしようとした場合は、図１４(ａ)に示すように、ブロック符号化部は、盗まれたパスワードを暗号鍵として本人以外の指紋データを暗号化し、認証サーバ装置側に送出することになる。

【０１２９】

これに応じて、認証サーバ装置に備えられた復号化部が、パスワード検索部から受け取ったパスワードに基づいて復号化処理を行うことにより、本人以外の指紋データが得られ、指紋データベースから検索された本人の標準データとともに、照合判定部による照合処理に供される。

この場合は、別人の指紋データを相互に比較することになるので、当然ながら、照合判定部により、明らかに不一致である旨の照合結果が得られ、この照合結果に応じて、図１３に示した認証制御部２６３は、この不当な利用者の利用資格を否認し、不正なアクセスとして排除すればよい。

【０１３０】

また、正当な資格を持つ利用者の指紋データが盗まれた場合にも、同様にして対処することができる。

この場合は、図１４(ｂ)に示すように、ブロック暗号化部は、誤ったパスワードを暗号鍵として、盗まれた指紋データを暗号化することになるから、認証サーバ装置に備えられた復号化部により、正当なパスワードを暗号鍵として復号化することによって、指紋データを復元する代わりに、無意味なビット列が生成されてしまう。

【０１３１】

したがって、照合判定部によって、このビット列と標準データとを照合すれば、明らかに不一致である旨の照合結果が得られ、これに応じて、図１３に示した認証制御部２６３は、この不当な利用者の利用資格を否認し、不正なアクセスとして排除すればよい。

このように、図１３に示した遠隔本人認証システムにおいては、利用者固有の特徴を示す生体情報と、利用者が他者から秘匿して管理すべきパスワードとの両方を本人の確認に用いるとともに、生体情報の揺らぎを利用して、認証情報の解読を困難にすることができる。

【０１３２】

ここで、生体情報は、測定の度に所定の誤差範囲内で変動しているために暗号化した場合にその解読が困難であり、この点は認証情報として優れている。その反面、生体情報が個人の生涯に渡って不変であるが故に、基本となる生体情報から測定誤差に相当する揺らぎを持った疑似生体情報を自由に作成可能な環境が構築されると、以降は該当する生体情報を認証情報として使用することが不可能となり、致命的な欠点となる可能性を含んでいる。

【０１３３】

一方、パスワードは、必要に応じて適宜変更が可能であり、認証情報としての使い勝手に優れている。その反面、従来の技術の項でも述べたように、非常に盗まれやすい上に、固定値であるために、パスワードを暗号化したとしても解読が容易である点が欠点である。

上述したように、生体情報とパスワードとを独立に見れば、それぞれの長所とともに短所を持っているが、図１３に示した本人認証システムによれば、生体情報とパスワードとを融合して分離を困難とすることにより、生体情報とパスワードとがそれぞれ有する長所短所を相互に補償して、利用者の資格の正当性を確実に確認することができる。

【０１３４】

これにより、パスワードの管理に関して利用者にかかる負担を軽減するとともに、遠隔本人認証システムの安全性を向上することが可能となり、ネットワークを介して重要な情報を安全に授受することができるので、ネットワークを介したショッピングシステムや秘匿性を必要とする情報をネットワークを介して授受するシステムを安全に機能させることができる。

【０１３５】

また、生体情報を公開鍵方式の暗号化方法によって暗号化してもよい。

この場合は、図１３に示した認証クライアント装置１０１において、ブロック暗号化部２５２は、後述する追加開示項６で述べる第３暗号化手段１４２として動作し、例えば、ＲＡＳアルゴリズムを用いて、依頼制御部２５１から受け取ったパスワードを秘密鍵として指紋データなどの生体情報を暗号化すればよい。

【０１３６】

また一方、図１３に示した認証サーバ装置１０２に備えられたブロック復号化部２６４は、後述する追加開示項６で述べる第３復号化手段１４７として動作し、認証制御部２６３を介して受け取った暗号化指紋データを公開鍵を用いて復号化し、復元された生体情報を照合処理に供すればよい。

この場合は、認証情報の暗号化に用いられた暗号鍵と復号化に用いられる暗号鍵とが異なっているので、例えば、認証サーバ装置１０２に対するハッキングによって、後述する追加開示項６で述べる資格情報登録手段１４４に相当するパスワードデータベース２６１の内容が盗まれたとしても、遠隔本人認証システム全体としての安全性を保証することができる。

【０１３７】

また、図１３に示した通信制御部４１３に代えてＩＣカードライタを備えて認

証クライアント装置を構成するとともに、通信制御部４２２に代えてＩＣカードリーダを備えて認証サーバ装置を構成し、ＩＣカードを認証情報を授受するための情報伝送媒体とする構成としてもよい。

【０１３８】

【発明の効果】

以上に説明したように、請求項１乃至請求項６の発明によれば、暗号化された生体情報を復号する際に、暗号化された生体情報に依存する暗号鍵を適用するので、生体情報の暗号化に用いた暗号化手法にかかわらず、暗号化生体情報の少なくとも一部が改竄されたときに、改竄の影響を復号結果全体に波及させ、元の生体情報とは全く異なるデータ列に変換することができる。

【０１３９】

一方、請求項７乃至請求項１２の発明によれば、暗号化処理に先立って、生体情報をスクランブルすることにより、暗号化生体情報を構成する各ブロックの内容を、生体情報を構成する複数のブロックの内容に依存させることができるので、暗号化生体情報が改竄された場合に、復号側において、改竄箇所に対する依存関係が形成された複数のブロックに渡ってその影響を拡大させ、元の生体情報とは大幅に異なるデータ列に変換することができる。

【０１４０】

請求項１３の発明によれば、生体情報とパスワードとを組み合わせることにより、互いの短所を補償するとともに、生体情報の揺らぎを利用して解析が困難な認証情報を認証処理に供することができるので、遠隔本人認証システムの安全性を向上することができる。

以上の説明に関して、更に、以下の項を開示する。

【０１４１】

追加開示項１．請求項３に記載の生体情報暗号化装置において、数値キー決定手段１１２は、生体情報に含まれる揺らぎ情報を抽出する揺らぎ抽出手段１２１と、揺らぎ抽出手段１２１から受け取った揺らぎ情報を対応する数値に変換し、変換結果を数値キーとして出力する数値変換手段１２２とを備えた構成であることを特徴とする。

【０１４２】

追加開示項１の発明は、揺らぎ抽出手段１２１および数値変換手段１２２の動作ににより、生体情報が揺らぎ情報を含んでいることを利用して無作為な数値キーを作成し、暗号鍵生成処理に供することができる。

特に、この追加開示項４の発明を適用することにより、生体情報が本来持っている揺らぎを利用して、暗号化の度に異なる暗号鍵を生成することができるので、乱数を発生させる機構を不要とすることができる。

【０１４３】

追加開示項２．請求項３に記載の生体情報暗号化装置において、制御情報作成手段１１５は、暗号化生体情報の入力に応じて、この暗号化生体情報を構成する各部分情報をそれぞれ反映した成分情報からなる要約情報を生成する要約手段１２３と、要約情報と数値キーとを所定の関数を用いて合成し、この合成結果を復号制御情報として作成手段１１６の処理に供する合成手段１２４とを備えた構成であることを特徴とする。

【０１４４】

追加開示項２の発明は、要約手段１２３の動作により、暗号化生体情報の各部分情報を反映した要約情報が得られるから、この要約情報と数値キーとに基づいて、合成手段１２４が動作することにより、暗号化生体情報を構成する各部分情報と復号制御情報とを確実に関連づけることができ、暗号化生体情報と復号制御情報とをより強固な依存関係によって結びつけることができる。

【０１４５】

この追加開示項２の発明を適用することにより、暗号化生体情報を構成する各ブロックの内容を一様に反映した復号制御情報を復号側に供給することができるので、後述する追加開示項４と組み合わせることにより、暗号化生体情報および復号制御情報のどの部分が改竄されたかにかかわらず、確実に暗号鍵を破壊することができる。

【０１４６】

追加開示項３．請求項３に記載の生体情報暗号化装置において、作成手段１１６は、暗号化生体情報と復号制御情報とを所定の規則に従って結合し、一体化し

た認証情報としてネットワーク送出する構成であることを特徴とする。

追加開示項３の発明は、作成手段１１６の動作により、暗号化生体情報と復号制御情報とを一体化した状態でネットワークを介して伝達することができるので、暗号化生体情報と復号制御情報とを個々に解析する作業を困難にし、暗号解読に対する防御性を高めることができる。

【０１４７】

追加開示項４．請求項４に記載の生体情報復号化装置において、数値キー復元手段１１８は、暗号化生体情報の入力に応じて、この暗号化生体情報を構成する各部分情報をそれぞれ反映した成分を用いて要約情報を生成する要約手段１２３と、復号制御情報から要約情報の寄与分を分離して、数値キーを復元する分離手段１２５とを備えた構成であることを特徴とする。

【０１４８】

追加開示項４の発明は、要約手段１２３によって得られた要約情報を分解手段１２５の処理に供することにより、追加開示項２の発明を適用した暗号化装置によって、暗号化生体情報に強固に結びつけられた復号制御情報から数値キーを復元し、暗号鍵生成手段１１３の処理に供することができる。

追加開示項５．請求項９に記載の生体情報暗号化装置において、スクランブル手段１３１は、変換対象の情報を構成する全ての要素の寄与分を変換後の各要素の値に反映する関数を用いて数値変換を行う構成であることを特徴とする。

【０１４９】

追加開示項５の発明は、スクランブル手段１３１による数値変換によって、暗号化生体情報の各ブロックが依存関係を持つ範囲を、元の生体情報の全てのブロックにまで拡大することができる。

この追加開示項５の発明を適用することにより、各ブロックが生体情報全体に依存する暗号化生体情報を生成するので、暗号化生体情報が改竄された場合に、復号側におけるスクランブル解除処理により、スクランブル解除結果を構成する全てのブロックに渡って改竄の影響を拡大し、元の生体情報とは大幅に異なるデータ列に変換することができる。

【０１５０】

追加開示項６．請求項１３に記載の遠隔本人認証システムにおいて、認証クライアント装置１０１に備えられた第３暗号化手段１４２は、パスワードを秘密鍵として、生体情報を暗号化する構成であり、認証サーバ装置１０２に備えられた資格情報登録手段１４４は、各利用者に対応するパスワードとして、該当する公開鍵を登録する構成であり、認証サーバ装置１０２に備えられた第３復号化手段１４７は、検索手段１４６から受け取った公開鍵を用いて、暗号化生体情報を復号化する構成であることを特徴とする。

【０１５１】

追加開示項６の発明は、認証クライアント装置１０１側で、第３暗号化手段１４２において、パスワードを秘密鍵として生体情報を暗号化し、認証サーバ装置１０２側では、資格情報登録手段１４４に登録された公開鍵を用いて、暗号化生体情報を復号化することにより、遠隔本人認証システムの安全性を更に向上することができる。

【０１５２】

特に、この追加開示項６の発明によれば、公開鍵方式の暗号化手法を採用することにより、認証サーバ装置に登録された資格情報が漏洩した場合にも、漏洩した情報に基づいて認証情報を作成することが不可能であるから、このような不正なアクセスを確実に排除することができる。

【図面の簡単な説明】

【図１】

請求項１および請求項２の発明の原理を示す図である。

【図２】

請求項３および請求項４の発明装置の原理ブロック図である。

【図３】

請求項７および請求項８の発明の原理を示す図である。

【図４】

請求項９および請求項１０の発明装置の原理ブロック図である。

【図５】

請求項１３の発明装置の原理ブロック図である。

【図６】

請求項３の暗号化装置および請求項４の復号化装置を適用した本人認証システムの構成図である。

【図７】

暗号化動作および復号化動作を表す流れ図である。

【図８】

認証情報の改竄が復号結果に及ぼす影響を説明する図である。

【図９】

請求項９の暗号化装置および請求項１０の復号化装置を適用した本人認証システムの構成図である。

【図１０】

スクランブルの効果を説明する図である。

【図１１】

生体情報照合処理の解析を防ぐ効果を説明する図である。

【図１２】

生体情報の構造解析を防ぐ効果を説明する図である。

【図１３】

請求項１３の遠隔本人認証システムの実施形態を示す図である。

【図１４】

不正アクセスを排除する動作を説明する図である。

【図１５】

従来の遠隔本人認証システムの構成例を示す図である。

【図１６】

生体情報を利用した本人認証システムの構成例を示す図である。

【図１７】

生体情報を照合する処理を説明する図である。

【図１８】

生体情報を利用した遠隔本人認証システムの構成例を示す図である。

【図１９】

生体情報の改竄による影響を説明する図である。

【符号の説明】

１０１、４１０　認証クライアント装置

１０２、４２０　認証サーバ装置

１１１　生体情報入力手段

１１２　数値キー決定手段

１１３　暗号鍵生成手段

１１４　第１暗号化手段

１１５　制御情報作成手段

１１６　作成手段

１１７　受取手段

１１８　数値キー復元手段

１１９　第１復号化手段

１２１　揺らぎ抽出手段

１２２　数値変換手段

１２３　要約手段

１２４　合成手段

１２５　分離手段

１３１　スクランブル手段

１３２　第２暗号化手段

１３５　第２復号化手段

１３６　スクランブル解除手段

１４１　資格情報入力手段

１４２　第３暗号化手段

１４３　出力手段

１４４　資格情報登録手段

１４５　入力手段

１４６　検索手段

１４７　第３復号化手段

１４８　照合手段

２１０、２３０　暗号化装置

２１１　ビットパターン作成部

２１２、２２７　暗号鍵生成部

２１３、２２６　一次鍵保持部

２１４、２３２、２５２、４１４　ブロック暗号化部

２１５、２２４　ハッシュ変換部

２１６　認証情報結合部

２１７、２２５　論理演算部

２２２　制御情報分離部

２２３、２４１、２６４　ブロック復号化部

２３１　離散フーリエ変換（ＤＦＴ）演算部

２３３、２４２　暗号鍵保持部

２３４　ＩＣカードライタ

２３５　ＩＣカードリーダ

２４３　逆離散フーリエ変換（ＤＦＴ）演算部

２５１、４１２　依頼制御部

２５３　認証情報作成部

２６１、４２４　パスワードデータベース

２６２　パスワード検索部

２６３、４０１、４２３　認証制御部

４０２、４１１　キーボード

４０３、４１５　ＣＲＴディスプレイ装置（ＣＲＴ）

４１３、４２２　通信制御部

４１６、４２５　時計

４３０　指紋データ測定装置

４３１　特徴抽出部

４３２　指紋読取部

４３３　指紋データ作成部

４４０　指紋照合装置

４４１　指紋データベース

４４２　指紋データ検索部

４４３、４４４　照合判定部

４４５　比較部

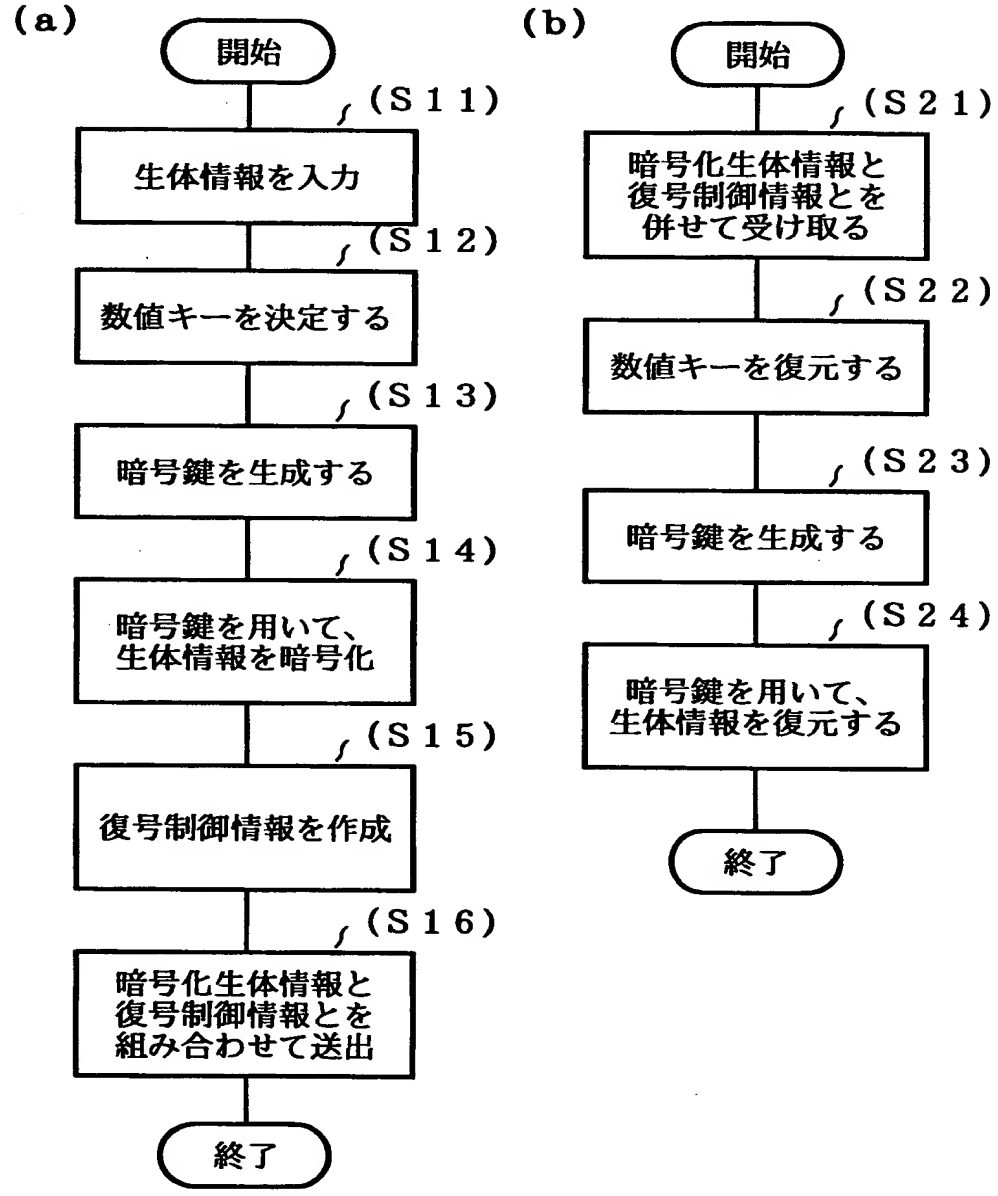
４４６　不正検出部

４４７　照合結果判定部

【書類名】　　図面

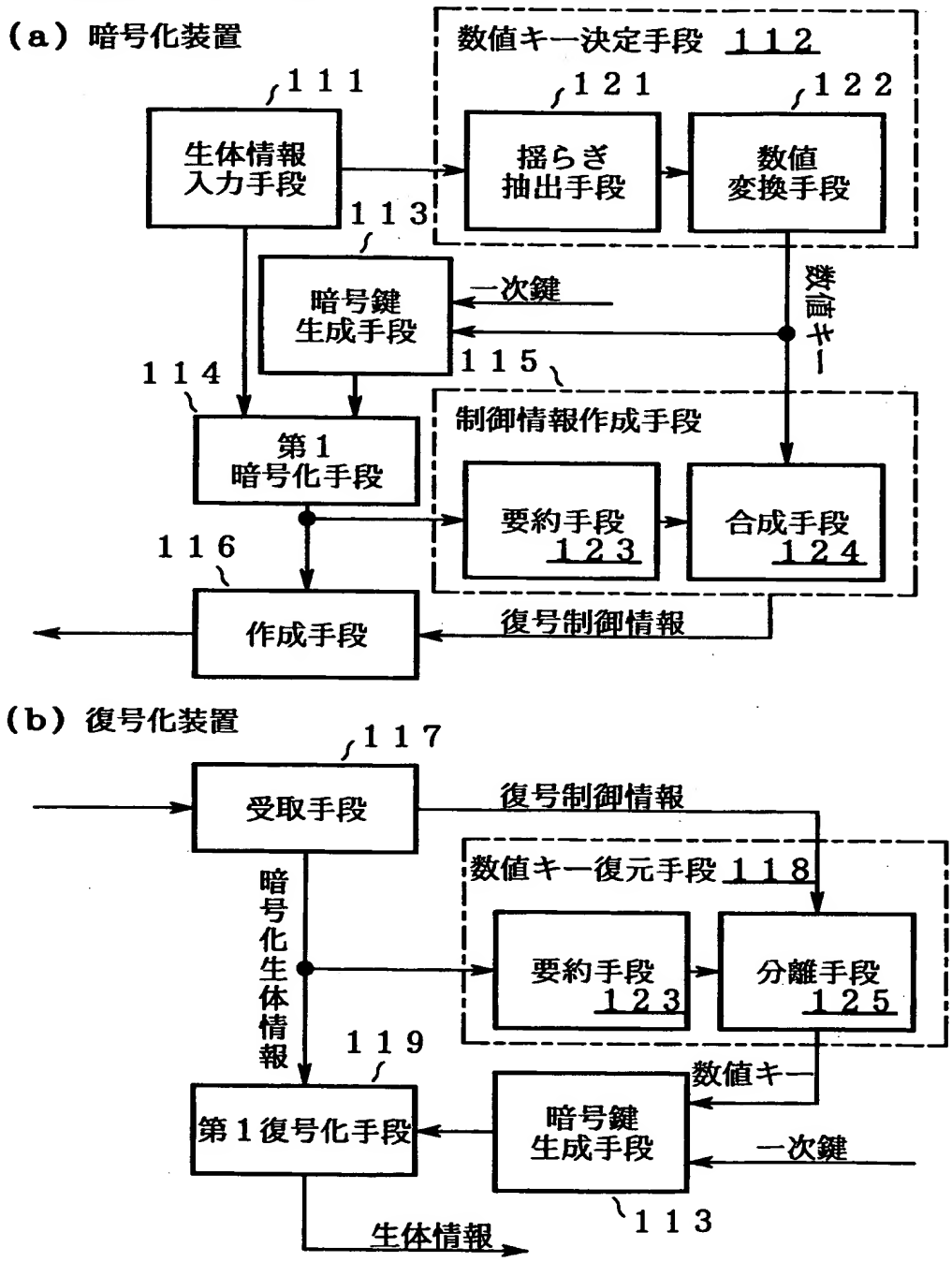
【図１】

請求項１および請求項２の発明の原理を示す図



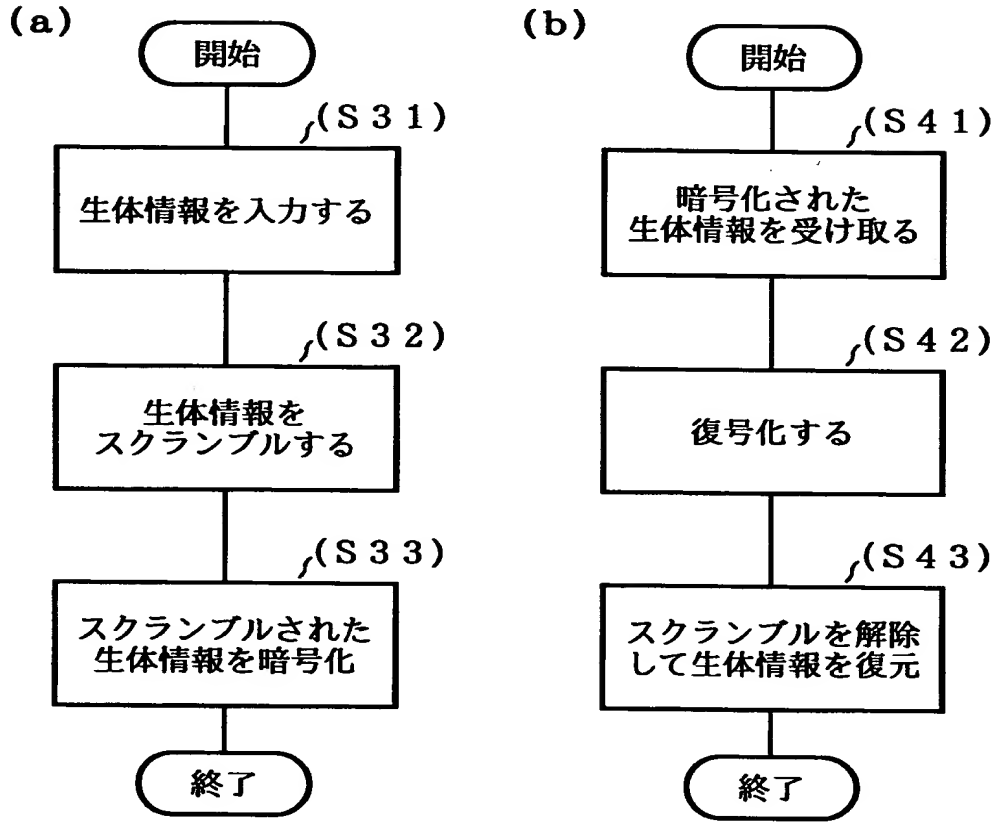
【図２】

請求項３および請求項４の発明装置の原理ブロック図



【図３】

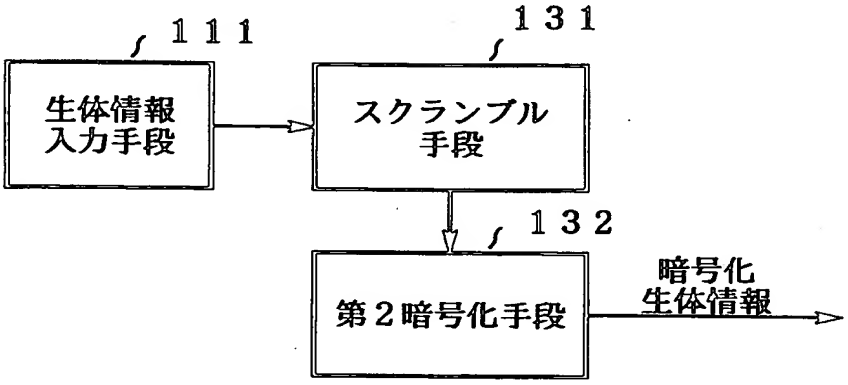
請求項７および請求項８の発明の原理を示す図



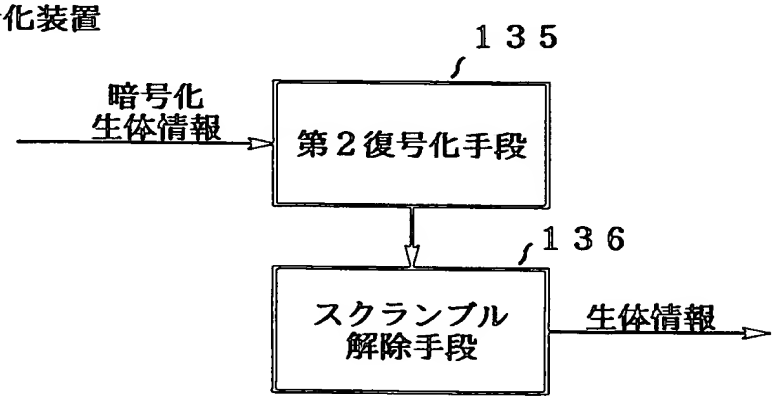
【図４】

請求項９および請求項１０の発明装置の原理ブロック図

（ａ）暗号化装置

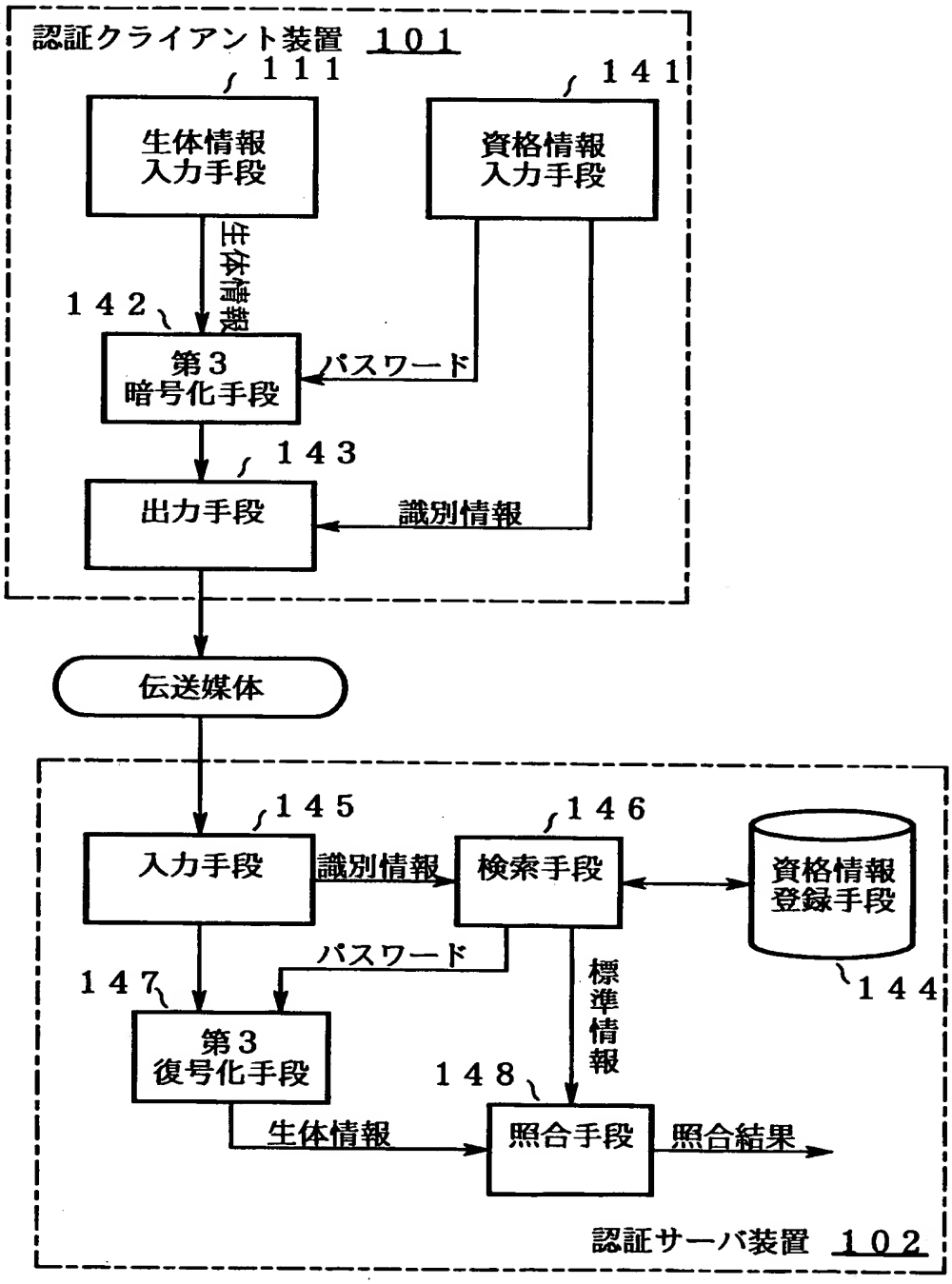


（ｂ）復号化装置



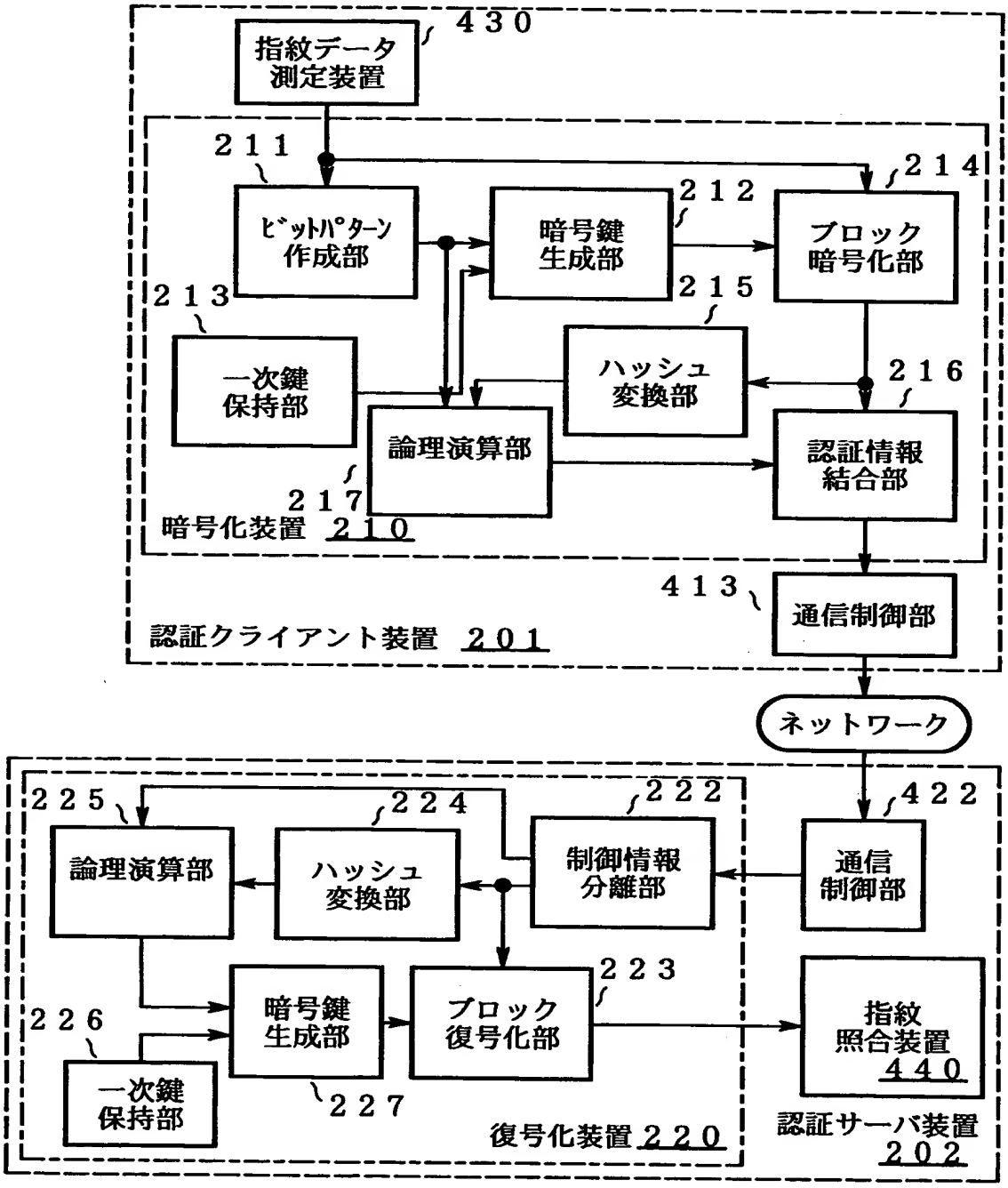
【図５】

請求項１３の遠隔本人認証システムの原理ブロック図



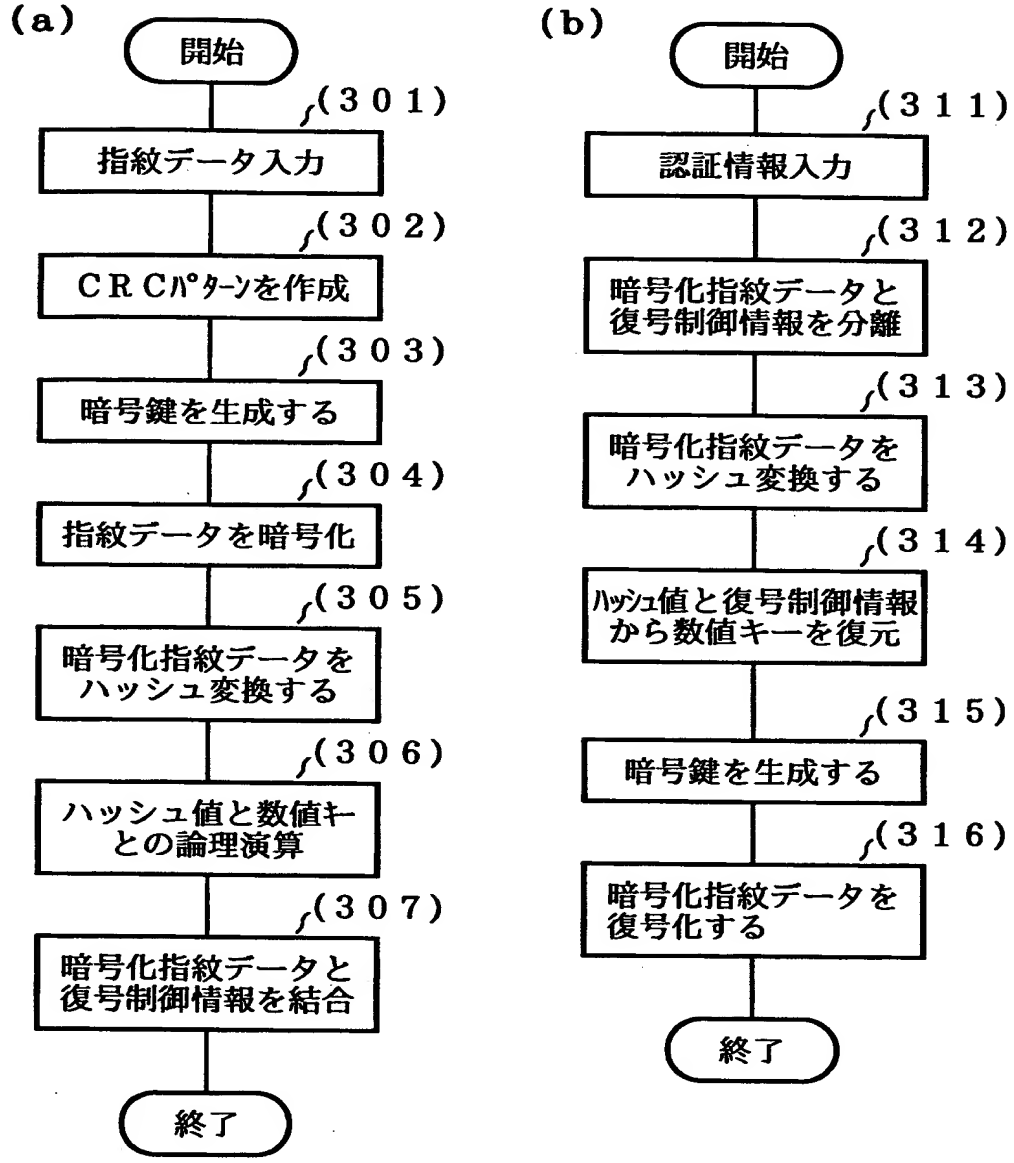
【図６】

請求項３および請求項４の発明を適用した本人認証システムの構成図



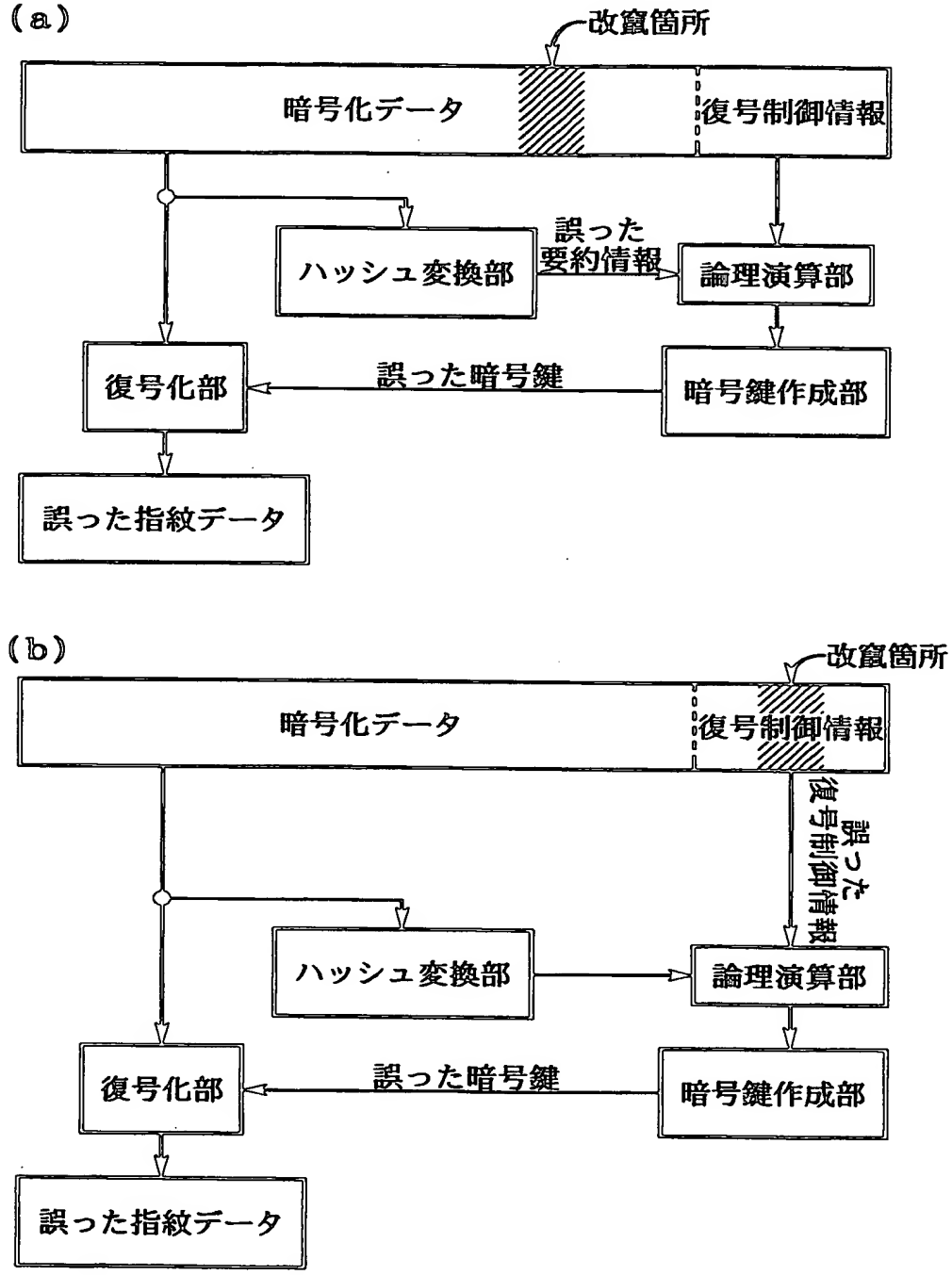
【図７】

暗号化動作および復号化動作を表す流れ図



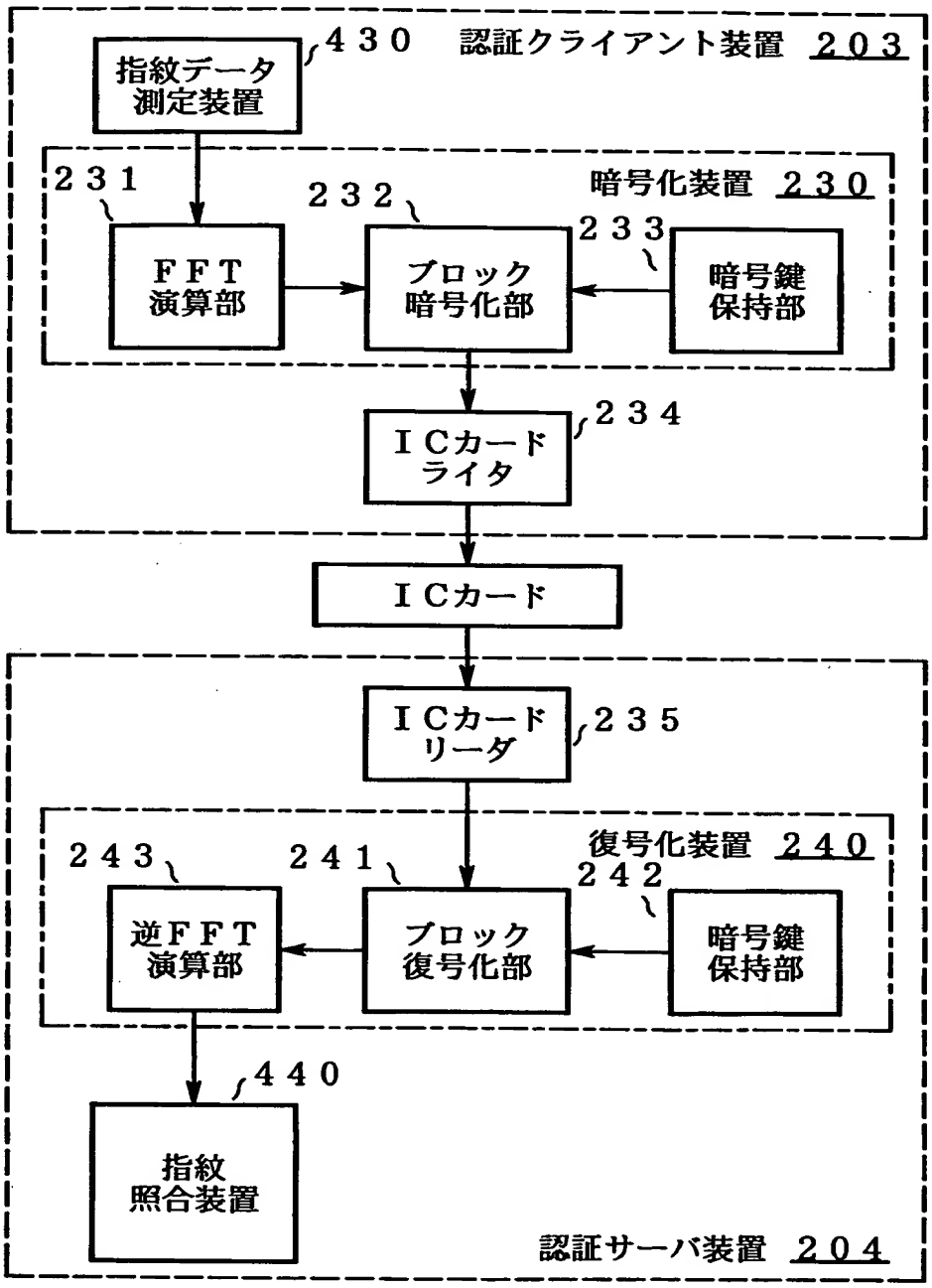
【図８】

認証データの改竄が復号結果に及ぼす影響を説明する図



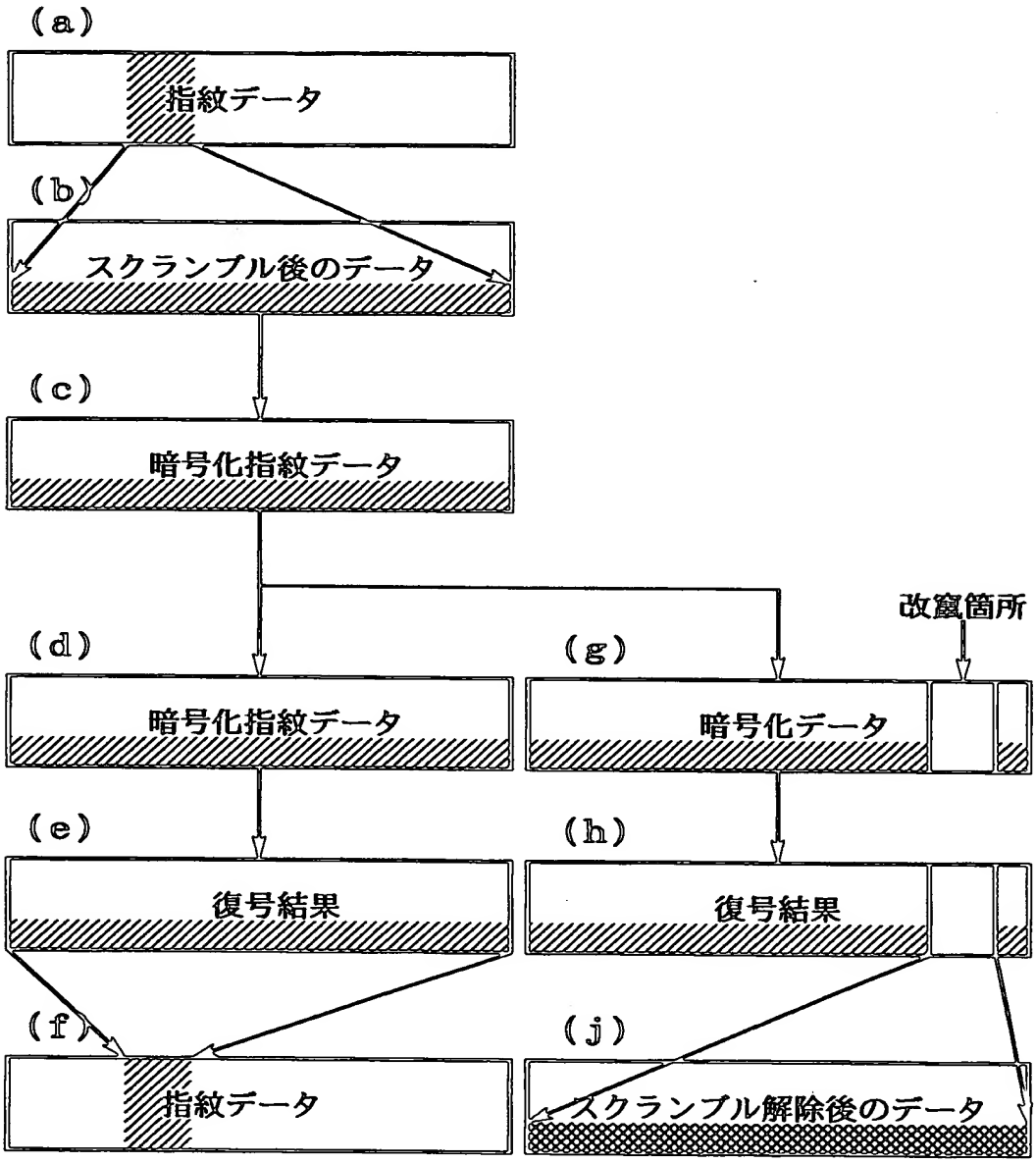
【図９】

請求項１３、１５の発明装置を適用した遠隔本人認証ｼｽﾃﾑの構成図



【図１０】

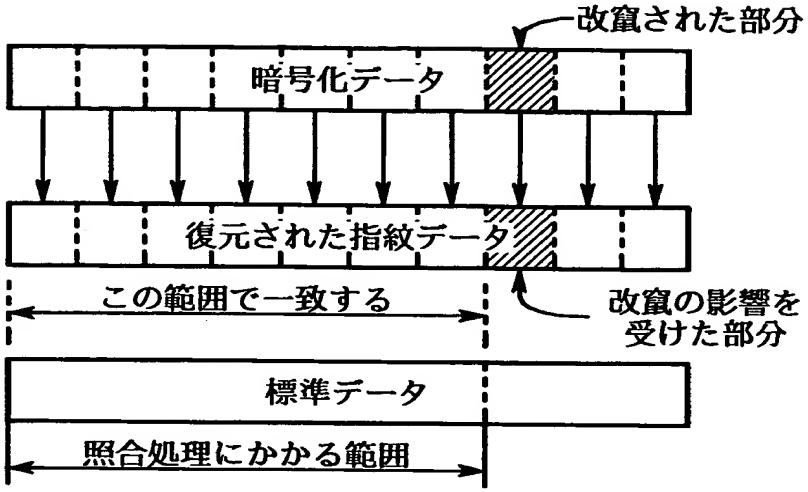
スクランブルの効果を説明する図



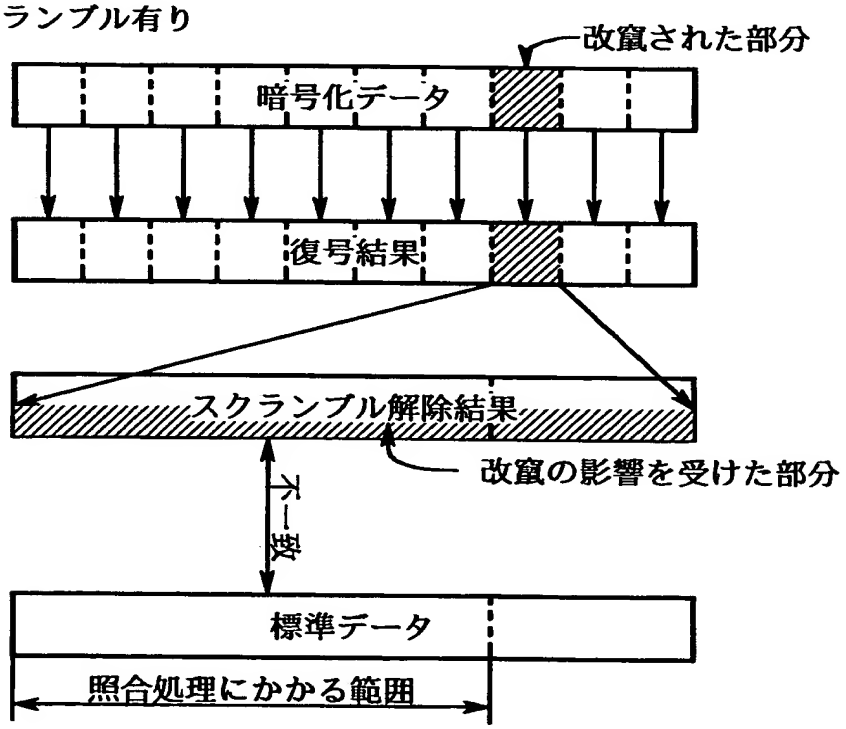
【図１１】

生体情報照合処理の解析を防ぐ効果を説明する図

（ａ）スクランブルなし

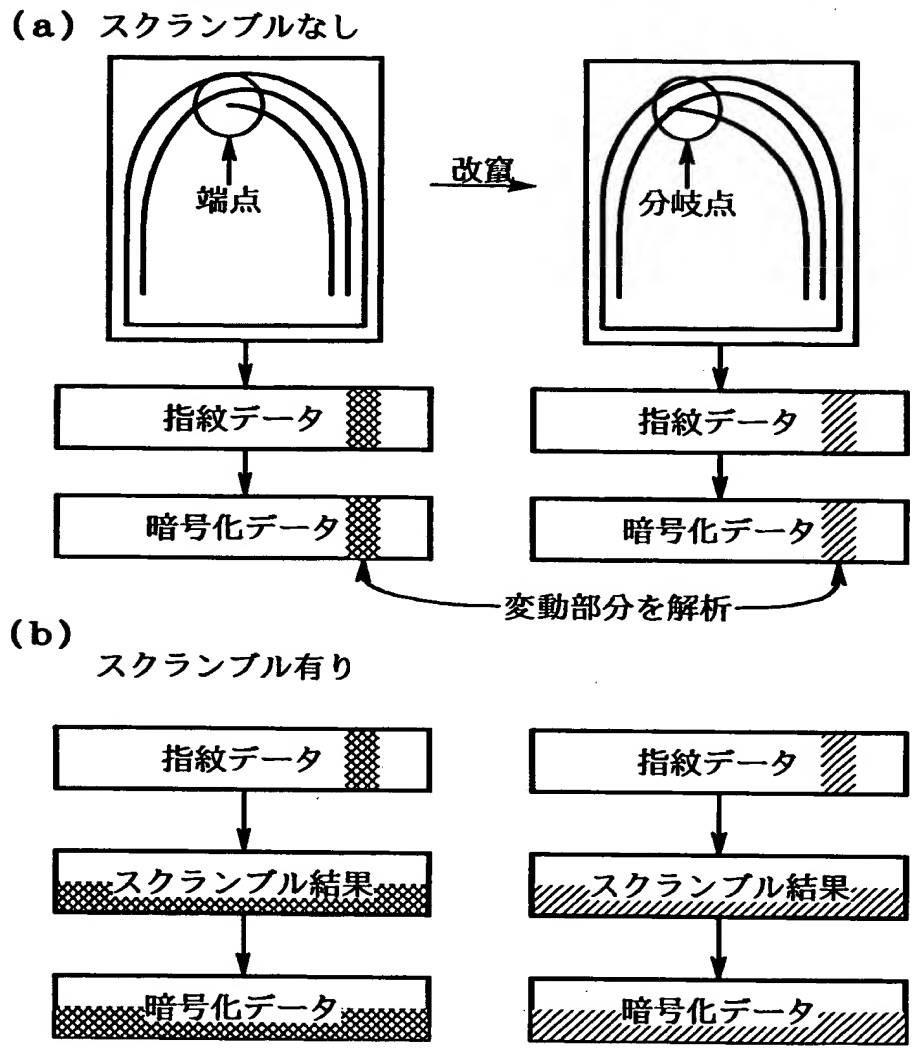


（ｂ）スクランブル有り



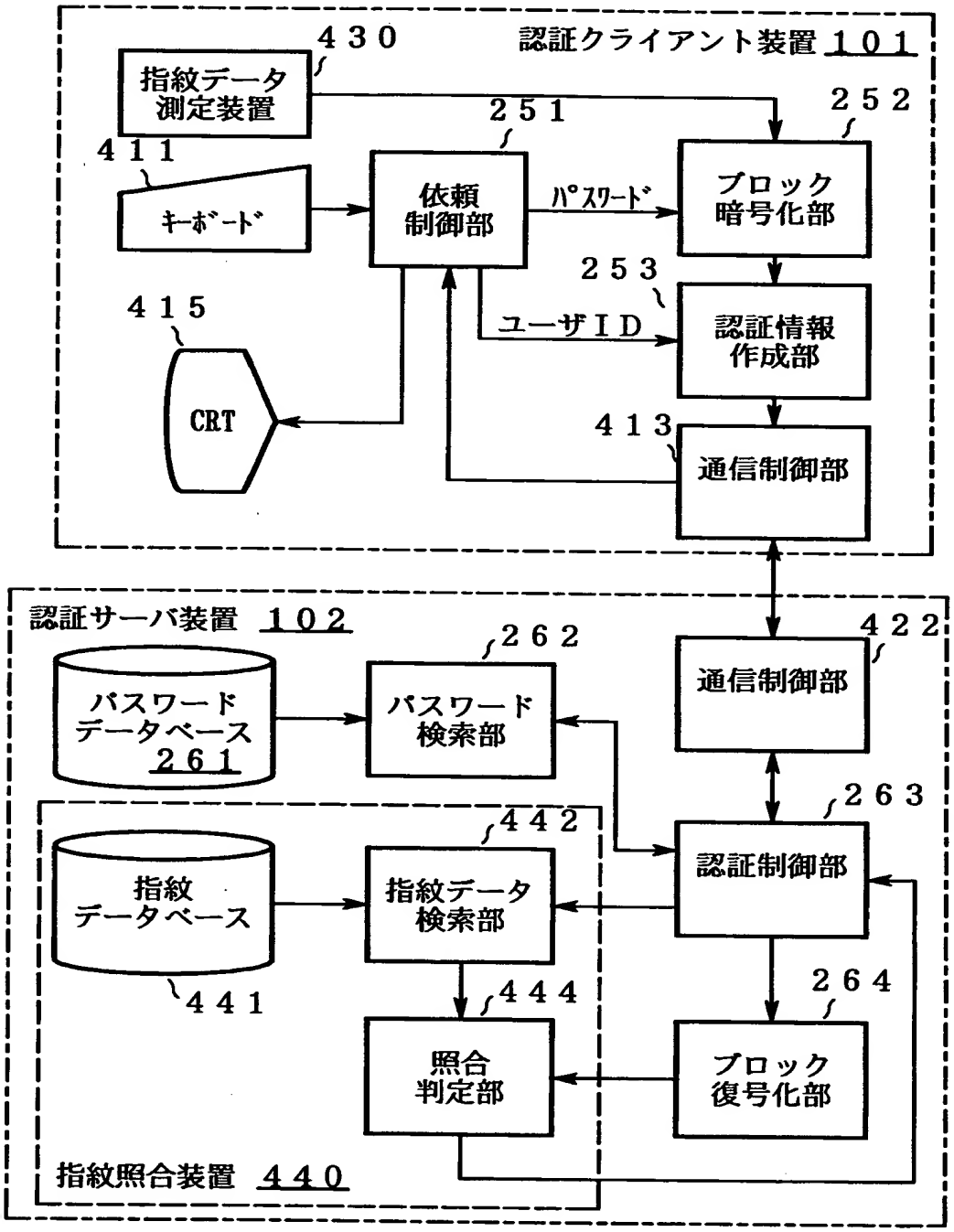
【図１２】

生体情報の構造解析を防ぐ効果を説明する図



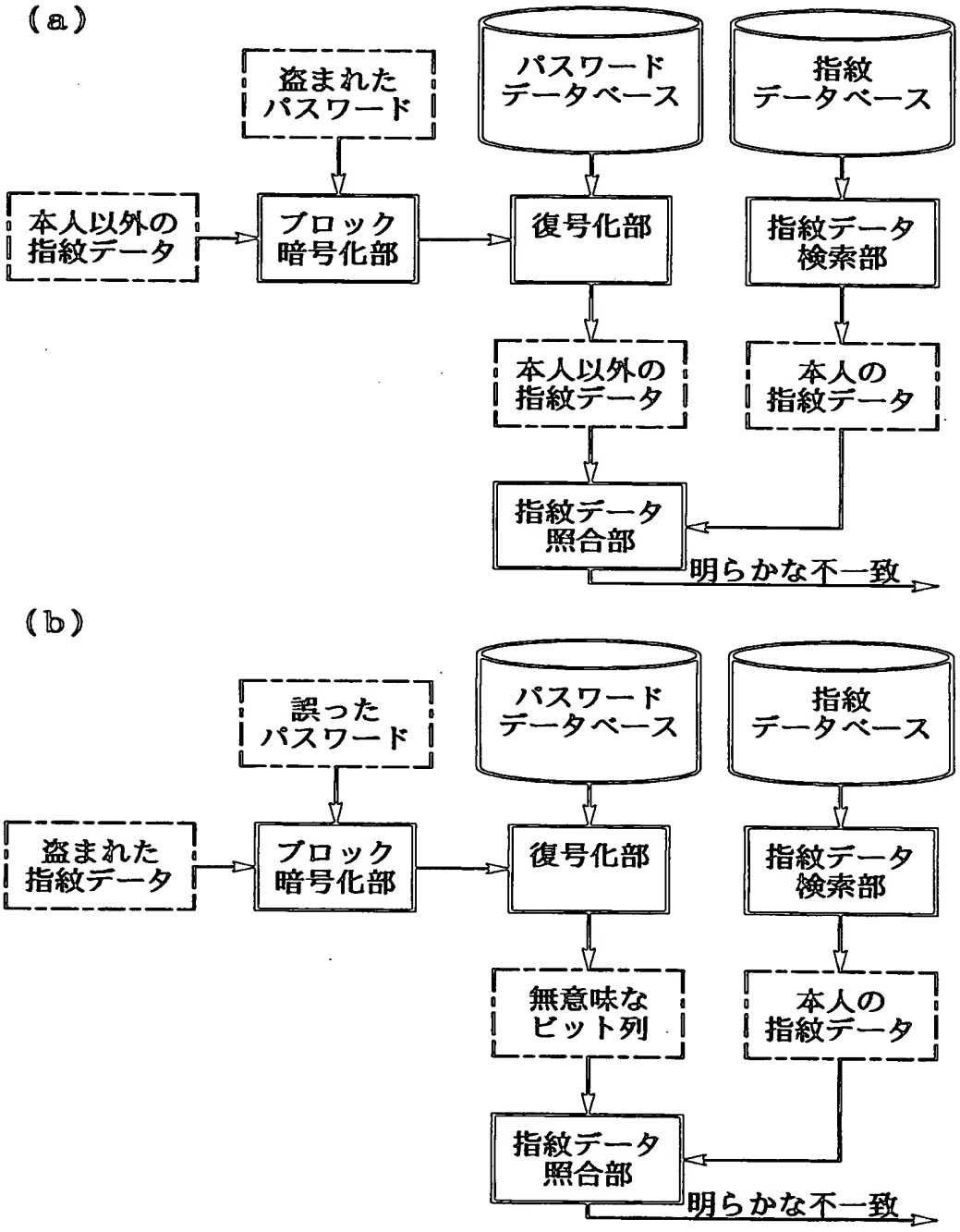
【図１３】

請求項１８の遠隔本人認証システムの実施形態を示す図



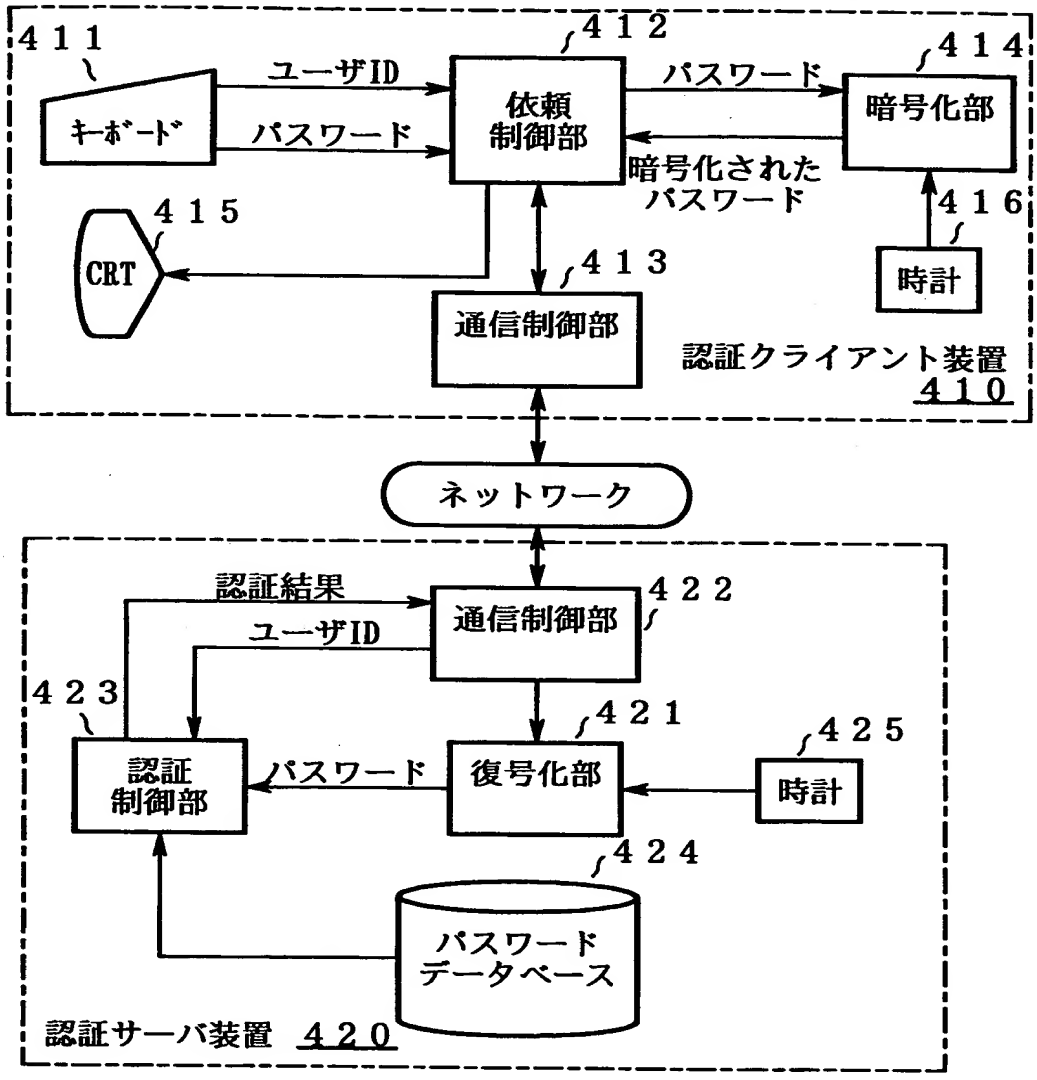
【図１４】

不正アクセスを排除する動作を説明する図



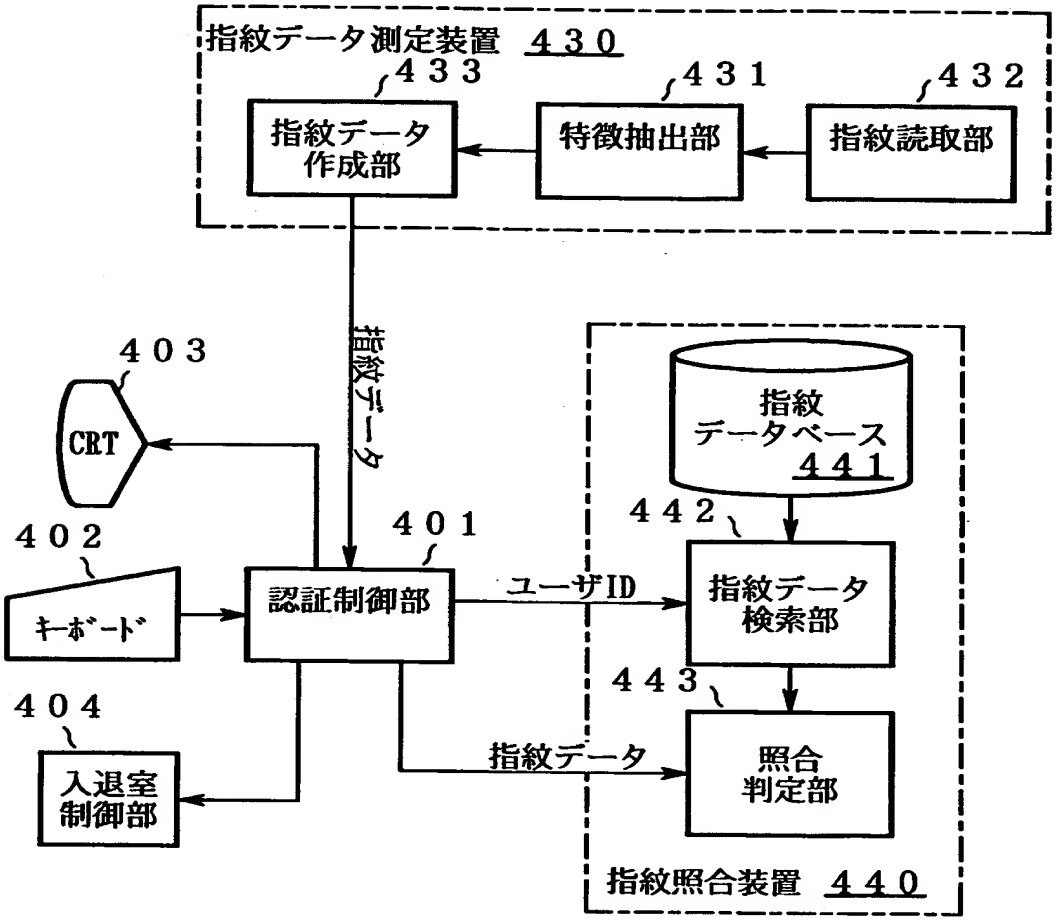
【図１５】

従来の遠隔本人認証システムの構成例を示す図



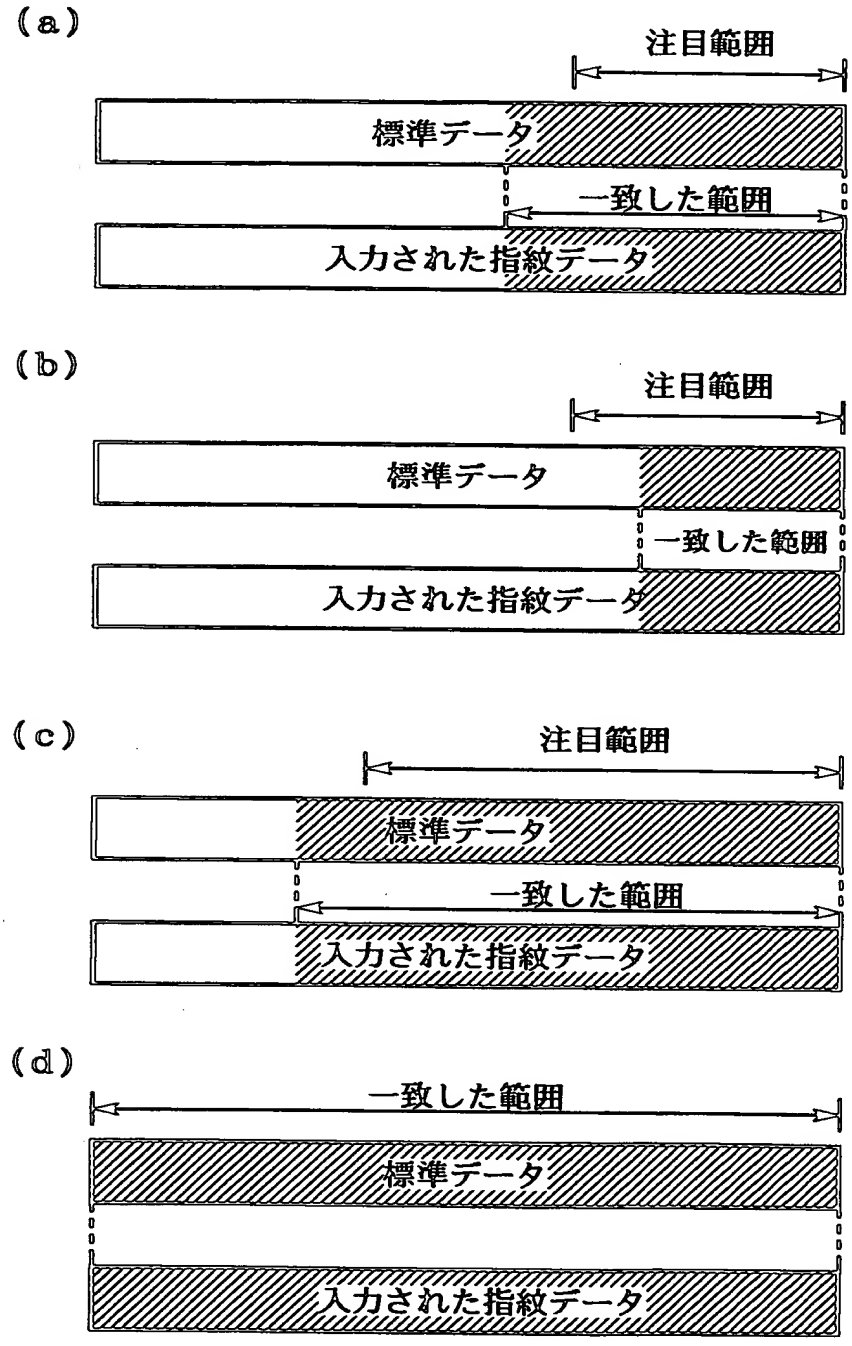
【図１６】

生体情報を利用した本人認証システムの構成例を示す図



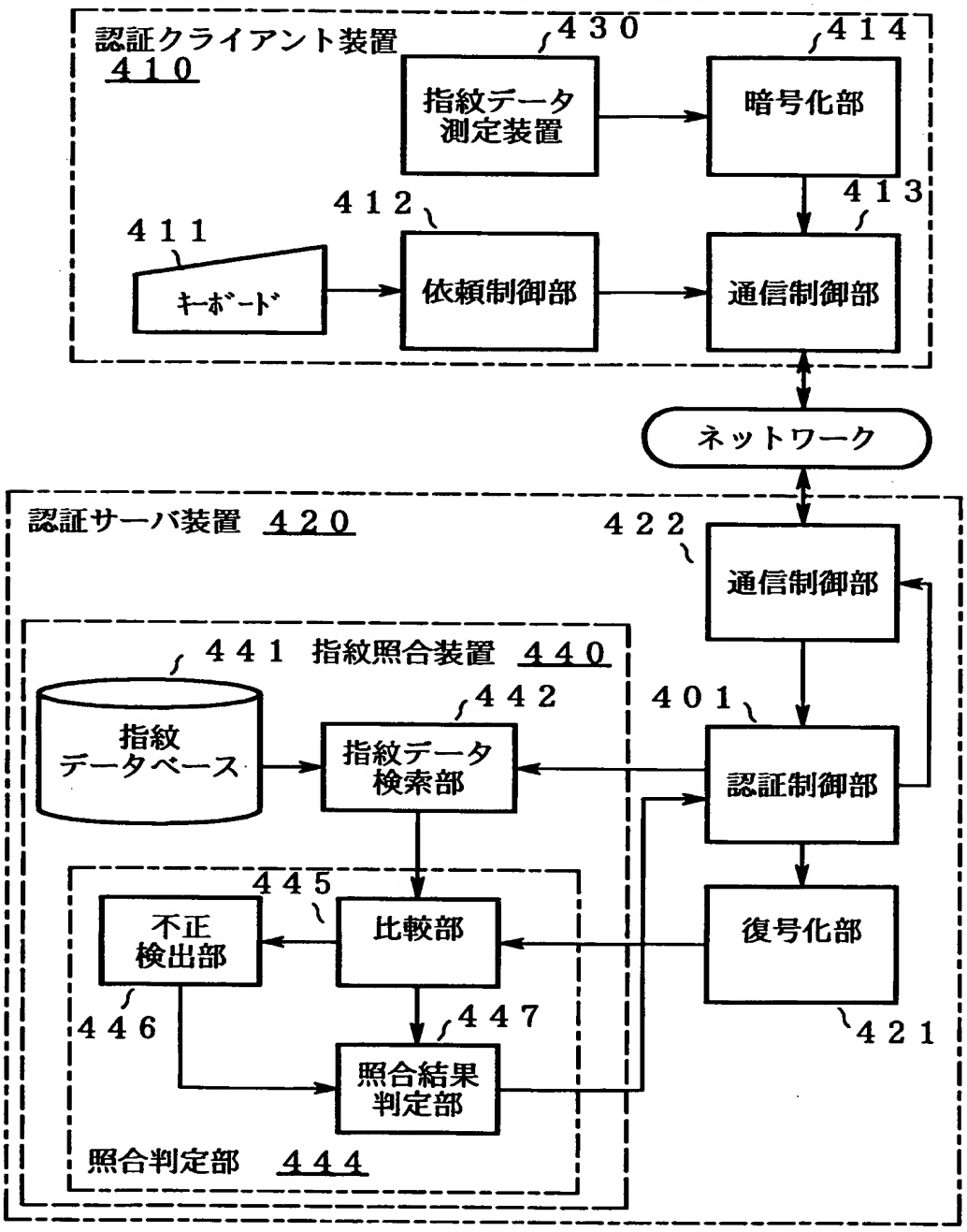
【図１７】

生体情報を照合する処理を説明する図



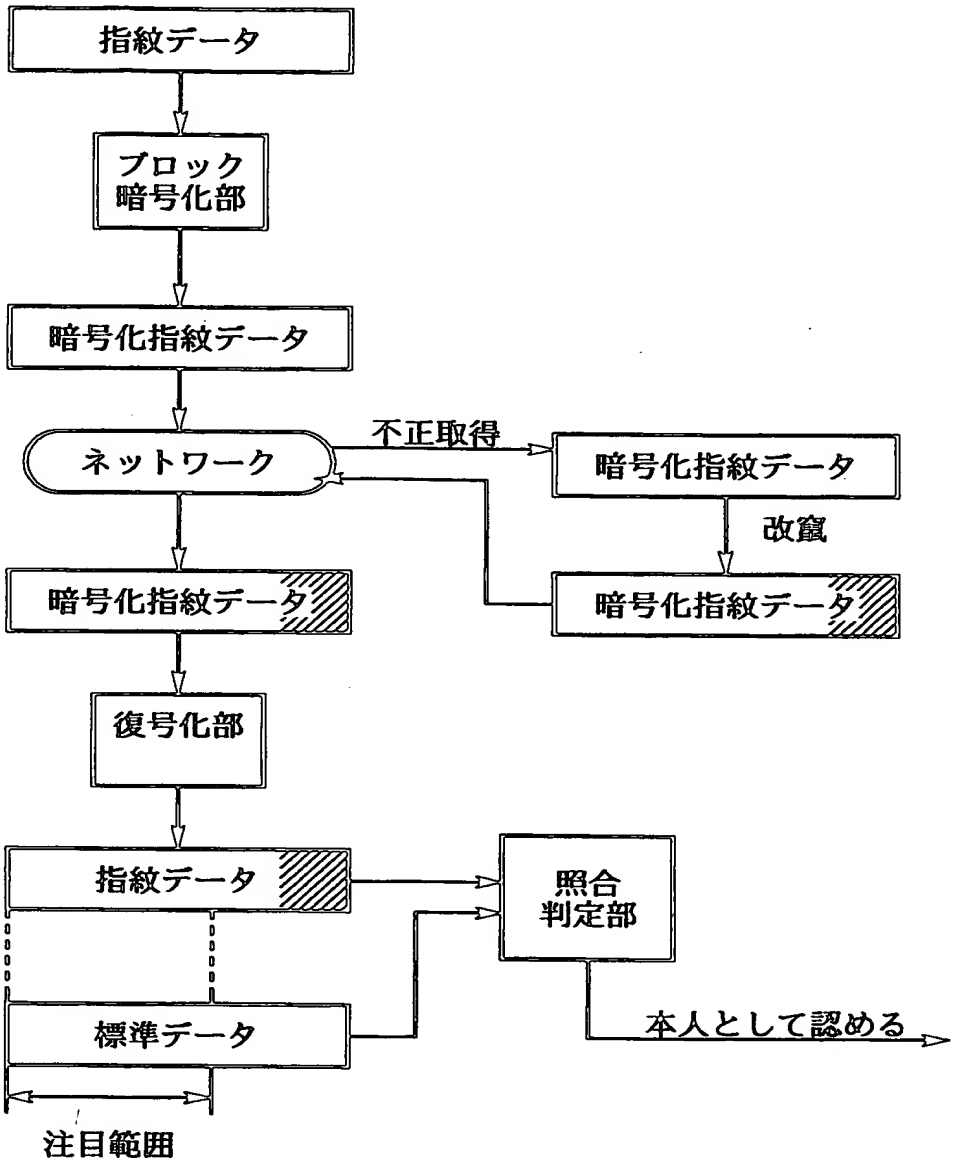
【図１８】

生体情報を利用した遠隔本人認証システムの構成例を示す図



【図１９】

暗号化生体情報の改竄による影響を説明する図



【書類名】　　要約書

【要約】

【課題】　本人を証明するための認証情報を安全かつ確実に伝達するための暗号化・復号化方法および装置並びに、生体情報の特徴を利用した遠隔本人認証システムを提供する。

【解決手段】　個人に固有の特徴を表す生体情報の入力を受け（Ｓ１１）、暗号化の都度、任意の値を持つ数値キーを決定し（Ｓ１２）、数値キーと所定の一次鍵とから暗号鍵を生成し（Ｓ１３）、暗号鍵を用いて生体情報を暗号化し（Ｓ１４）、得られた暗号化生体情報と数値キーとに基づいて、復号化処理側で暗号鍵を再生するための復号制御情報を作成し（Ｓ１５）、暗号化生体情報と復号制御情報とを組み合わせて認証情報を作成する（Ｓ１６）。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社